Installation and Reference Guide

HP StorageWorks Secure Path V3.0D for Sun Solaris

Product Version: 3.0D

Ninth Edition (July 2004)

Part Number: AA–RKYDK–TE

This guide describes the HP StorageWorks Secure Path for Sun Solaris software. It includes information about Secure Path technology, installation procedures, and management commands.

Secure Path V3.0D for Sun Solaris Installation and Reference Guide
Ninth Edition (July 2004)
Part Number: AA–RKYDK–TE

Contents

Figures

Tables

About this Guide

This installation and reference guide provides information to help you:

- Understand Secure Path technology
- Determine hardware and software prerequisites
- Install Secure Path software
- Manage Secure Path using `spmgr`
- Contact Technical support for additional assistance

"About this Guide" topics include:

Overview

This section covers the following topics:

Intended audience

This book is intended for use by system administrators who are experienced with any of the following:

- Sun Solaris operating systems
- RA8000
- ESA12000
- EMA16000
- MA8000
- EMA12000
- EVA5000
- EVA3000

Related documentation

In addition to this guide, HP provides the *HP StorageWorks Secure Path v3.0D for Sun Solaris Release Notes.*

Conventions

Conventions consist of the following:

- Document conventions
- Text symbols
- Equipment symbols

Document conventions

This document follows the conventions in Table 1.

Table 1: Document conventions

Convention	Element
Blue text: Figure 1	Cross-reference links
Bold	Menu items, buttons, and key, tab, and box names
Italics	Text emphasis and document titles in body text
`Monospace font`	User input, commands, code, file and directory names, and system responses (output and messages)
`Monospace, italic font`	Command-line and code variables
Blue underlined sans serif font text (http://www.hp.com)	Web site addresses

Text symbols

The following symbols may be found in the text of this guide. They have the following meanings:

WARNING: Text set off in this manner indicates that failure to follow directions in the warning could result in bodily harm or death.

Caution: Text set off in this manner indicates that failure to follow directions could result in damage to equipment or data.

Tip: Text in a tip provides additional help to readers by providing nonessential or optional techniques, procedures, or shortcuts.

Note: Text set off in this manner presents commentary, sidelights, or interesting points of information.

Equipment symbols

The following equipment symbols may be found on hardware for which this guide pertains. They have the following meanings:

Any enclosed surface or area of the equipment marked with these symbols indicates the presence of electrical shock hazards. Enclosed area contains no operator serviceable parts.

WARNING: To reduce the risk of personal injury from electrical shock hazards, do not open this enclosure.

Any RJ-45 receptacle marked with these symbols indicates a network interface connection.

WARNING: To reduce the risk of electrical shock, fire, or damage to the equipment, do not plug telephone or telecommunications connectors into this receptacle.

Any surface or area of the equipment marked with these symbols indicates the presence of a hot surface or hot component. Contact with this surface could result in injury.

WARNING: To reduce the risk of personal injury from a hot component, allow the surface to cool before touching.

Power supplies or systems marked with these symbols indicate the presence of multiple sources of power.

WARNING: To reduce the risk of personal injury from electrical shock, remove all power cords to completely disconnect power from the power supplies and systems.

Any product or assembly marked with these symbols indicates that the component exceeds the recommended weight for one individual to handle safely.

WARNING: To reduce the risk of personal injury or damage to the equipment, observe local occupational health and safety requirements and guidelines for manually handling material.

Rack stability

Rack stability protects personnel and equipment.

WARNING: To reduce the risk of personal injury or damage to the equipment, be sure that:

- The leveling jacks are extended to the floor.
- The full weight of the rack rests on the leveling jacks.
- In single rack installations, the stabilizing feet are attached to the rack.
- In multiple rack installations, the racks are coupled.
- Only one rack component is extended at any time. A rack may become unstable if more than one rack component is extended for any reason.

Getting help

If you still have a question after reading this guide, contact an HP authorized service provider or access our web site: http://www.hp.com.

HP technical support

Telephone numbers for worldwide technical support are listed on the following HP web site: http://www.hp.com/support/. From this web site, select the country of origin.

Note: For continuous quality improvement, calls may be recorded or monitored.

Be sure to have the following information available before calling:

- Technical support registration number (if applicable)
- Product serial numbers
- Product model names and numbers
- Applicable error messages
- Operating system type and revision level
- Detailed, specific questions

HP storage web site

The HP web site has the latest information on this product, as well as the latest drivers. Access storage at: http://www.hp.com/country/us/eng/prodserv/storage.html. From this web site, select the appropriate product or solution.

HP authorized reseller

For the name of your nearest HP authorized reseller:

- In the United States, call 1-800-345-1518
- In Canada, call 1-800-263-5868
- Elsewhere, see the HP web site for locations and telephone numbers: http://www.hp.com.

Secure Path Technology

HP StorageWorks Secure Path is a server-based software product that enhances StorageWorks RAID array storage systems by providing automatic recovery of data from server-to-storage system connection failures. Secure Path supports multiple I/O paths between host and storage, which improves overall data availability. If any component in a path between host and storage fails, Secure Path redirects pending and subsequent I/O requests to an alternate path.

This chapter provides the following Secure Path information:

Overview

Secure Path is a high-availability software product that manages and maintains continuous data access to the following StorageWorks storage systems:

- RA8000
- ESA12000
- EMA16000
- MA8000
- EMA12000
- EVA5000
- EVA3000

Secure Path eliminates the RAID controller, HBA, and interconnect hardware (cables, switches, and connectivity devices) as single points of failure in the I/O path.

By using redundant hardware and advanced RAID technology, Secure Path enhances fault tolerance and storage system availability by providing automated failover capability.

Redundant physical connections define separate physical *paths* in a Secure Path hardware configuration. Each path originates at an HBA port on a server, and ends at a unique RAID controller port in the storage system.

Figure 1 illustrates basic Secure Path hardware configurations. The physical connections define two separate paths. Each path originates at a unique SAN host bus adapter on a Solaris server and ends at a port on a separate RAID controller on the storage system.

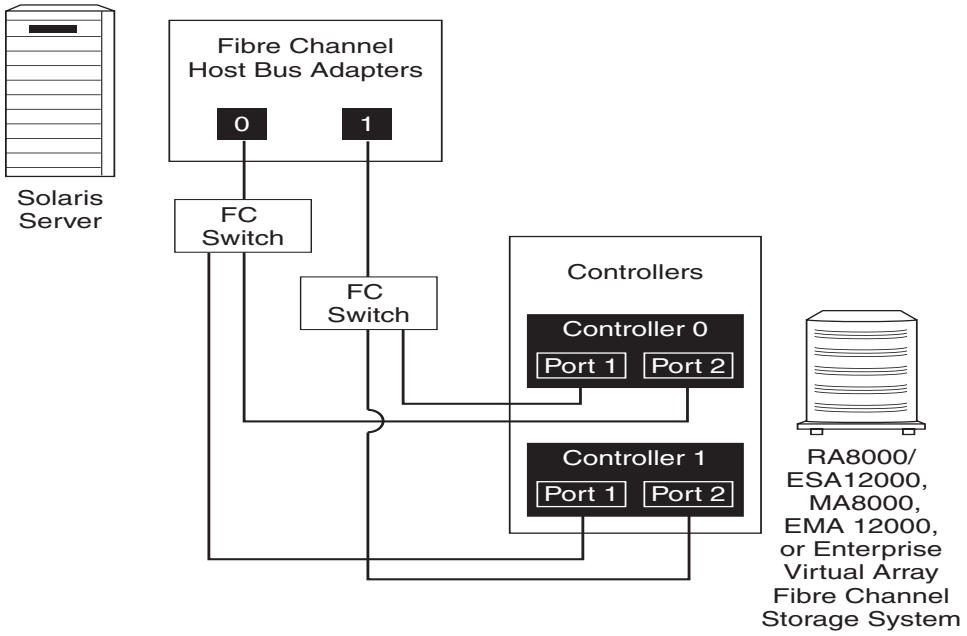

Figure 1: Basic Secure Path Fibre Channel configuration

Secure Path enables dual StorageWorks RAID controllers to operate in an active/active LUN ownership implementation, referred to as dual-redundant multiple-bus mode. Multiple-bus mode allows each controller to process I/O independently of the other controller under normal operation. A path consists of a unique connection from adapter to device. I/O is active on one path at a time and storage units (LUNs) may be moved between paths using the Secure Path Management Tool `spmgr`.

Secure Path takes advantage of the HSG80/HSV110/HSV100 preferred path unit attribute. Available storage units are preferred to one or the other of the two controllers by setting a preferred path unit attribute. This attribute determines which controller is used for access at storage system boot time. During runtime, storage units may be moved between paths at any time through the use of the Secure Path Management utility. On HSG80/HSV110/HSV100 RAID storage systems, storage units may also be accessed on each controller through either of two available ports.

The Secure Path software detects the failure of I/O operations on a failed path and automatically reroutes traffic to other available paths. Secure Path software seeks alternate paths through available SAN switches, controllers, controller ports, and host bus adapters. Path failover is completed seamlessly, without process disruption or data loss.

Following replacement of a failed adapter, cable, controller, or attached components, storage units can be restored or failed back to their original path using the Secure Path Management utility.

To protect against drive failure in a Secure Path environment, storage units can be configured using RAID Levels 0+1, 1, or 5.

Features

Secure Path provides the following features

- StorageWorks dual-controller RAID systems and host servers equipped with multiple HBAs allows redundant physical connectivity along independent Fibre Channel fabric paths
- Monitors each path and automatically re-routes I/O to a functioning alternate path if a component failure occurs
- Determines the availability of storage units and physical paths through path verification diagnostics
- Monitors and identifies failed paths and failed-over storage units
- Facilitates static load balancing which allows manual movement of devices between paths.
- Facilitates four dynamic load balancing algorithms based on I/O type.
- Automatically restores failed over storage units to repaired paths with auto failback capability enabled
- Implements anti-thrash filters to prevent failover/failback effects caused by marginal or intermittent conditions
- Maximizes data throughput and bandwidth using dual RAID controllers configured in multiple-bus mode operation with load balancing capability enabled
- Detects failures reliably without inducing false or unnecessary failovers
- Implements failover/failback actions transparently without disrupting applications
- Provides remote management commands that allow the local Secure Path configuration to be managed from a remote client system.

Software components

This section describes the Secure Path software kit for Solaris software components.

Drivers

The following Secure Path drivers manage paths to a storage device while providing a single device target to applications.

- **swsp driver—**A failover driver that is presented as a pseudo-HBA driver to system SCSI disk drivers. This driver presents multiple paths as a single device to the host SCSI disk driver. It also initiates path failover when necessary and manages all kernel threads related to failover.
- **hsx driver—**An array-specific driver that provides paths from an HBA driver for specific arrays up to the `swsp driver`. This driver manages the separate paths to a LUN and encapsulates array-specific knowledge, such as specific commands to migrate a LUN from one controller to the other. The `hsx driver` supports StorageWorks HSG and Enterprise Virtual Array controllers.
- **path driver—**Required by the Solaris operating system to allow the hsx and swsp drivers to communicate in the kernel.

Figure 2 illustrates the driver model structure.

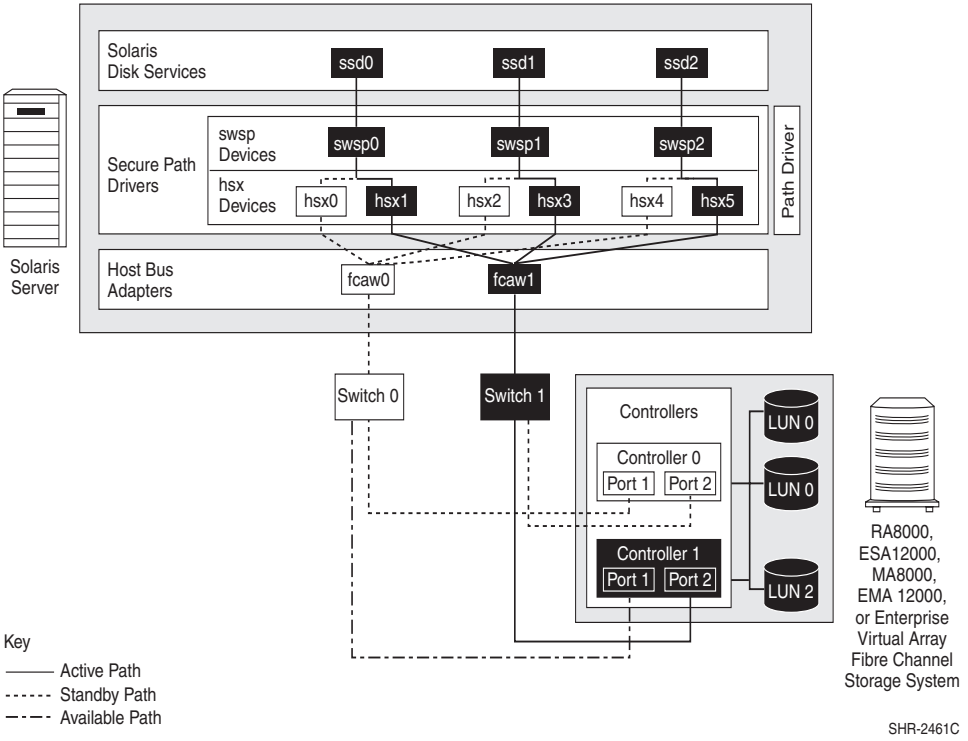

Figure 2: Driver model structure

Agent

The Secure Path agent (`spagent`) is a daemon process that provides an interface for Secure Path applications and utilities to communicate to the multipath drivers. The `spagent` also provides notification of path change events through e-mail. The `spagent` is not required to be running for Secure Path drivers to configure and provide full failover functionality. However, it must be running if e-mail event notification is desired. The only supported method to start and stop the Secure Path agent is the `spinit` script.

Running spagent in single-user mode

Secure Path v3.0D allows `spagent` to run when the Sun server is running in single-user mode. Be aware of the following limitations when running in single-user mode:

- Ensure that network services are configured and running properly or `spmgr` will fail at startup.
- If you switch from multi-user mode to single-user mode, `spagent` terminates. You must use the `spinit start` command to manually start `spagent`, once you are running in single-user mode.

Starting/Stopping spagent

Do not start or kill `spagent` directly—always use the `spinit` command to start and stop the agent.

The proper syntax to start `spagent` is:

```
/etc/init.d/spinit start
```

The proper syntax to stop `spagent` is:

```
/etc/init.d/spinit stop
```

Management tools

Secure Path Manager (`spmgr`) is a command line application that allows you to monitor and manage Secure Path devices, and to change the configuration settings of the drivers. See Chapter 4 for a complete description of `spmgr` commands.

Note: You must have network services running in order for *spmgr* to communicate with *spagent*.

Configuration tool

The Secure Path configuration utility, `spconfig`, is run after installing Secure Path and performs the following functions:

- Queries storage systems
- Enables you to modify the Secure Path storage configuration
- Modifies driver configuration files for Secure Path

Controller ownership

Storage systems that are multiple-bus capable generally contain a pair of redundant controllers and support one of the following basic operational models:

- **Active/passive**—In the active/passive model, all storagesets are assigned ownership to one controller of the pair for I/O processing. The other controller is inactive, but available as a substitute in case of failure on the original.
- **Active/active**—In the active/active model, I/O processing may be routed through both controllers simultaneously, providing better performance and high availability. The RAID arrays supported by Secure Path implement a modified version of the active/active model. Although I/O can be processed simultaneously by both controllers, any given storageset is *owned* or online to a host through only one controller.

  Ownership of a storageset may be transferred to the other controller at any time through a host-initiated command sequence. However, because the ownership transfer results in controller cache flushing and I/O wind-down, the storageset may become inaccessible for a period of several seconds. Arbitrary ownership transfers are never automatically initiated by Secure Path and should be avoided.

Note: Secure Path automatically retries I/O requests that terminated in error due to ownership transfers. It also queues new I/O requests until the ownership transfer has completed, to ensure data integrity.

Path definition

Within Secure Path, a path is defined as the collection (configuration) of physical interconnect components, including HBAs, switches, cables, RAID controllers, and the ports on the controllers. Because the Secure Path driver component is positioned between the HBA driver and the system SCSI disk driver, the Secure Path driver can only distinguish physical paths when elements of the SCSI equivalent address are different.

Some configurations include multiple switches within a fabric, with the switches connected by one or more inter-switch links. Secure Path cannot detect these paths and cannot manage them. While these inter-switch paths provide an additional level of redundancy within the fabric, their management is handled directly within the switch. Refer to the documentation received with your switch hardware for more information about inter-switch link routing and failover policies.

Secure Path automatically sets the path state and reflects the status of the current actual path. Because of path failures, the currently active path may be different from what you expect. See Table 3 on page 30 for descriptions of path states and attributes.

Secure Path operation

Path failover occurs automatically when a selected set of error conditions is detected. Secure Path normally performs path failover only when user I/O is active or if path verification is enabled. However, it is possible for Secure Path Manager to show some units with a common failed path in the failover state, while other units remain accessible through that path. Units remain in the failed path if there is no I/O or until they are polled.

Failover follows a hierarchy, conditioned by the state of load balancing, as described below. Secure Path does not change the mode of Preferred paths in failover situations, so you can restore original path assignments after making repairs.

- Load balancing disabled:

  When a failure occurs, Secure Path marks the path Failed and switches to the next Available path connected to the same controller, if there is one.

  If there is no Available path on the same controller, Secure Path attempts to move the device to a Standby path on the other controller.

- Load balancing enabled:

  When a failure occurs, Secure Path marks the affected path as Failed. This removes it from the list of usable paths for the storageset.

  — If there are other Active paths, Secure Path continues to Load Balance across those paths.

  — If no other Active paths remain on the same controller, Secure Path moves the device to a Standby path on the other controller, marks all available paths on that controller as Active, and continues to Load Balance across those Active paths.

  — If no Active paths remain for the device, Secure Path activates an Available path on the same controller, if one exists.

  — If no Available paths remain on the same controller, Secure Path attempts to move the device to a Standby path on the other controller.

Failback options

Secure Path lets you set the path failback option to *Manual* or *Automatic*.

- In manual mode, you must enter a management utility command to restore devices to their preferred path. The operation is performed even if system I/O is in process to the selected device.

- In *Automatic* mode, Secure Path tests a failed path at fixed intervals if I/O is in process for the affected device. If the path appears to be viable, and the path is set as Preferred, the path state is set to Active and I/O will again be routed through this path.

Load Balancing

When enabled, load balancing allows multiple paths between a host and a specific storageset to be used in one of four load balancing algorithms. Using multiple paths spreads the load across all components in the RAID storage system and maximizes performance.

Load balancing may not be used in environments that use device reservations as a lock mechanism because, the RAID array controllers enforce reservations on a per-port basis.

Load balancing requires a Fibre Channel configuration that results in at least four unique paths from the host node to the storage system. While this can be accomplished with several different physical configurations, maximum performance potential is achieved when all four ports of the RAID storage system are used.

When load balancing is enabled, the Secure Path driver causes all paths to the owning controller to be marked Active by default. This is true when any of the following conditions occurs:

- A host boots up
- Secure Path fails over a storageset from one controller to the other
- You manually move a selected storageset between controllers using the Secure Path management utility, `spmgr`

Table 2 lists Dynamic load balancing types and a description of each type.

Table 2: Dynamic load balancing types

Dynamic load balancing type	Description
Round Robin	Rotates through all available paths on the active controller with equal distribution to each
Least Service Time	Uses the available path on the active controller that has the lowest outstanding I/O bytes count
Least I/O	Uses the available path on the active controller that has the fewest outstanding I/O requests
Least Bandwidth	Uses the available path on the active controller which takes the least average time to complete a command

Path Verification

When enabled with `spmgr`, path verification causes Secure Path to periodically test the viability of all paths to all storagesets for paths marked Available, Failed, Active, or Standby. Path verification does not test paths that are in a Quiesced state.

Path verification is useful for detecting failures that affect overall path redundancy, before they affect failover capability. If an Active path fails path verification, failover occurs. If an Available path fails path verification, its state will change from Available to Failed.

If a path marked Failed passes path verification, the path state is set to Available if it is on the Active controller, and Standby if it is on the Standby controller. If auto failback is enabled, the path becomes Active only if the path is on the Active controller and it is marked Preferred.

Path management behavior summary

Table 3 provides a summary of the path management behavior of Secure Path.

Table 3: Path management behavior summary

Feature	Behavior/Action
Startup	1. Chooses the Preferred path to the controller on which the LUN is online. 2. Marks the Preferred path Active. If no path is marked Preferred, select one and make it the Active Path.
Active Path Failure	■ Marks the Active path as Failed and fails to the Available path. ■ Redirects I/O through available paths. ■ If there are no Available paths, failover occurs to a Standby path on the other controller.
Available or Standby Path Failure	■ Performs path verification ■ Marks failed path as Failed
Path Repaired	■ Marks the path Available or Standby depending on which controller the device is currently online to. ■ If Auto Restore is enabled, and the path is preferred, then that path is marked Active.

Secure Path Parameter Defaults

Table 4 shows the Secure Path default values enabled during installation.

Table 4: Secure Path installation default values

Parameter	Default value
Autorestore	off
Load balancing	off
Path verification	on
Verification period	30 Seconds
Preferred paths	None
Console event log messages	Critical

Table 4: Secure Path installation default values

Parameter	Default value
Syslog event log messages	Critical, Warning
Mail event log messages	Critical, Warning, Informational
Mail event log e-mail	Enabled to send to the root account

The `spmgr` utility can be used to customize your configuration. Refer to "Managing Secure Path" on page 67 for information about `spmgr` customization.

Hardware Setup

2

This chapter provides the following Secure Path hardware setup information:

Hardware setup overview

The following procedure presents an overview of the hardware setup.

1. Ensure that all users have logged off the server and all array file systems have been backed up and unmounted, prior to setting up your hardware.
2. Verify that all the following hardware and software prerequisites have been met:
   - Supported HBAs are installed and working properly.
   - Supported version of Solaris, with all required patches, is loaded.

Note: Refer to the *HP StorageWorks Secure Path v3.0D Release Notes* for all hardware and software prerequisites.

---

3. Configure your StorageWorks RAID array.
4. Cable your HBAs, switches, and storage, making sure that the configuration is valid.

This guide describes only one basic Secure Path configuration. Many other valid configurations are possible; however, they are not documented here. Therefore, before installing Secure Path on a new or existing Fibre Channel (FC) configuration, first review the *HP StorageWorks SAN Design Reference Guide* found on the HP website. The guide familiarizes you with various high availability connection layouts for FC devices and cabling.

For the most current reference guide, visit the HP website at http://www.hp.com/country/us/eng/prodserv/storage.html

Verifying required components

Before installing Secure Path software, verify that you have received the Secure Path software kit and the FC hardware that you ordered for this installation. If you are missing any components, please contact your account representative or call HP Global Services at 1-800-354-9000. Refer to the *HP StorageWorks Secure Path v3.0D for Sun Solaris Release Notes* for the basic requirements of Secure Path operation.

Installing and configuring the storage systems

The following two sections describe the steps required for installing and configuring RAID systems and Sun servers for Secure Path operation in fabric (FC-SW) mode, one section for StorageWorks Enterprise Virtual Array storage systems and one section for setting up HSG80-based storage systems.

Before proceeding, you should have all Fibre Channel adapters installed in your Sun server. If required, power down your server and install the Fibre Channel adapters according to the adapter installation instructions. Reboot your server and ensure that the adapters are functioning before proceeding.

- If you are using Enterprise Virtual Array storage, follow the procedure described in "Configuring StorageWorks Enterprise Virtual Arrays" on page 36 for setup instructions.
- If you are using HSG80-based storage, follow the procedure described in "Configuring StorageWorks MA8000/EMA12000 RAID Arrays" on page 38.

For instructions on connecting your storage to your server and preparing to install Secure Path, follow the procedure described in "Connecting storage to the server" on page 41.

Configuring StorageWorks Enterprise Virtual Arrays

This section provides the steps required to install and configure HSV110/HSV100-based storage arrays.

Before beginning, record the following host information:

- LAN name of the host
- Host IP address
- List of the Fibre Channel adapter World Wide Names that will be configured with the arrays.

Note: The HBA World Wide Names (WWPNs) may not be available or known at this time. If this is the case, step 2, step 3, and step 4 cannot be performed. Those steps are completed in Chapter 3, "Installing Secure Path Software" on page 43.

Access the Command View EVA management appliance from a supported web browser, such as Internet Explorer or Netscape Navigator.

Before your host servers can use the virtual disks, ensure that you have the following completed:

Note: Refer to the online help system for Command View EVA or the *StorageWorks Management Appliance Element Manager for Enterprise Only User Guide* for information on these procedures. All of these procedures need to be completed for your host to use the virtual disks.

---

1. **Initialize the storage system and create disk groups**. When you first view the Enterprise Virtual Array from the Element Manager software, the storage pool is presented as *uninitialized storage*. Follow documented procedures for initializing the storage system and creating disk groups in your element manager user documentation.
2. **Add the host to the storage system**. Before the host can use the storage system's virtual disks, it must be known to the storage system. Adding the host creates a path from the storage system to one host adapter.
3. **Add ports to all host adapters**. From the Host Properties Page, choose **Add Port** to add connections to the remaining HBAs.
4. **Create and present virtual disks to the host**. Follow the steps for "Creating a Virtual Disk Family" in your element manager user documentation to create the virtual disk family, create virtual disks, and present the disks to the host.

Several options are available for selecting a path preference and mode for a virtual disk. To optimize load balancing the load should be evenly distributed between controller A and controller B. The boot default selected controller may be chosen by setting the controller *Preferred path/mode*. It is recommended that either **Path A - Failover only** or **Path B - Failover only** be used. This mode allows Secure Path to control failback to the original controller following a controller failure and replacement.

Note: **Path A—Failover/failback** and **Path B—Failover/failback** are not supported on Secure Path for Sun Solaris. That feature is designed for operating systems that cannot run Secure Path.

Configuring StorageWorks MA8000/EMA12000 RAID Arrays

This section provides the steps to install and configure HSG80-based storage arrays.

Caution: If you are installing Secure Path on an existing RAID storage system, stop **all** I/O to the RAID system and skip steps 1 and 2 below. For each RAID system in a production environment being converted to Secure Path operation, also make sure that all users have logged off the Sun Solaris servers. Follow normal procedures to back up the storage systems before proceeding.

1. Unpack the RAID system and install the PCMCIA cards in the controllers.
2. Power on the RAID system. Allow the cache batteries to charge, if necessary, before proceeding.
3. Establish a serial connection to the RAID storage system and use the CLI utility to configure the RAID system and create storagesets, as required.

Caution: Before proceeding, allow initialization of the storagesets to complete.

Note: Secure Path installation requires that at least one LUN be configured on the RAID storage system, but a complete disk/device configuration is strongly recommended. Additionally, the units must be visible to at least two paths from the Solaris Server using *format*.

4. Verify the configuration of the RAID system by entering either of the following commands:

```
CLI> show this_controller
CLI> show other_controller
```

An example of the controller output (with reference line numbers appended) follows.

```
Controller:                                                    1.
        HSG80 ZG90305234 Software V87F-3, Hardware E08         2.
        NODE_ID          = 5000-1FE1-0000- 8920                3.
        ALLOCATION_CLASS = 0                                   4.
        SCSI_VERSION     = SCSI-2                              5.
        Configured for MULTIBUS_FAILOVER with ZG90811309       6.
            In dual-redundant configuration                    7.
        Device Port SCSI address 6                             8.
        Time: 01-AUG-2000  09:39:19                            9.
        Command Console LUN is disabled                       10.
Host PORT_1:                                                  11.
        Reported PORT_ID = 5000-1FE1-0000-8923                12.
        PORT_1_TOPOLOGY = FABRIC (fabric up)                  13.
       Address          = 021000                              14.
Host PORT_2:                                                  15.
        Reported PORT_ID = 5000-1FE1-0000-8924                16.
        PORT_2_TOPOLOGY = FABRIC (connection down)            17.
NOREMOTE_COPY                                                 18.
Cache:                                                        19.
        128 megabyte write cache, version 0012                20.
        Cache is GOOD                                         21.
        No unflushed data in cache                            22.
        CACHE_FLUSH_TIMER = DEFAULT (10 seconds)              23.
Mirrored Cache:                                               24.
        128 megabyte write cache, version 0012                25.
        Cache is GOOD                                         26.
```

```
        No unflushed data in cache                              27.
Battery:                                                        28.
        NOUPS                                                   29.
        FULLY CHARGED                                           30.
        Expires:                            16-DEC-2003         31.
```

a. Configure the RAID system controllers for Multiple-bus Failover Mode, if the controllers are in Transparent Failover Mode (see line 6 of the example controller output). This procedure is documented in Appendix B.

   In Transparent Failover mode, under fabric configuration, both left-hand ports share the same WWPN. Similarly, both right-hand ports share the same WWPN.

Note: When you change the HSG80 controller pair from Transparent Failover Mode to Multiple-bus Failover Mode in fabric, the WWPN for the different host ports are all unique. This information is necessary when using the */opt/HPfcraid/config.sh* utility to assign the WWPN to target mapping for configuring the new adapters

For example, in Transparent Failover Mode, host port 1 has a WWPN of 5000-1FE1-0000-8921. This is the same for the top and bottom controllers. When the controllers are configured for Multiple-bus Failover Mode, the WWPN for port 1 of the top controller will change to 5000-1FE1-0000-8923, while host port 1 of the lower controller will have a WWPN of 5000-1FE1-0000-8921. The target to WWPN map must reflect these different values.

---

b. Set the preferred path, if desired, for each storage unit to specify the controller that the unit will use upon the RAID system boot time as follows:
   Enter the following command to obtain a list of all units defined in the RAID storage system:

```
CLI> show units full
```

An example of the show units output follows:

```
D11                                              DVGRPR0     (partition)
   LUN ID:      6000-1FE1-0000-8920-0009-9030-5234-006E
   NOIDENTIFIER
   Switches:
    RUN                   NOWRITE_PROTECT        READ_CACHE
     READAHEAD_CACHE         WRITEBACK_CACHE
     MAXIMUM_CACHED_TRANSFER_SIZE = 32
   Access:
           ALL
   State:
     ONLINE to this controller
     Not reserved
     NOPREFERRED_PATH
   Size:              8533749 blocks
   Geometry (C/H/S): (1680 / 20 / 254)
```

As shown in this example, the state of the unit is online to `this_controller` and no preferred path has been assigned.

c. Enter the following commands to specify the preferred path for each of the units:

```
CLI> set (unit #) preferred_path = this_controller
```

- or -

```
CLI> set (unit #) preferred_path = other_controller
```

Example:

```
CLI> set d11 preferred_path = other_controller
```

d. Enter the following CLI commands to transition the units to the preferred path:

```
CLI> restart other_controller
CLI> restart this_controller
```

Connecting storage to the server

This section describes how to connect configured storage to your server. For more information on supported configurations, access the HP website at: http://www.hp.com/country/us/eng/prodserv/storage.html.

1. Cable the Fibre Channel adapter and the RAID storage system controllers to the SAN Switches and HBAs, as shown in Figure 3 on page 42.

2. Proceed to Chapter 3 on page 43 to install Secure Path.

Note: You must map WWPNs before installing Secure Path as described in "Installing Secure Path Software" on page 43.

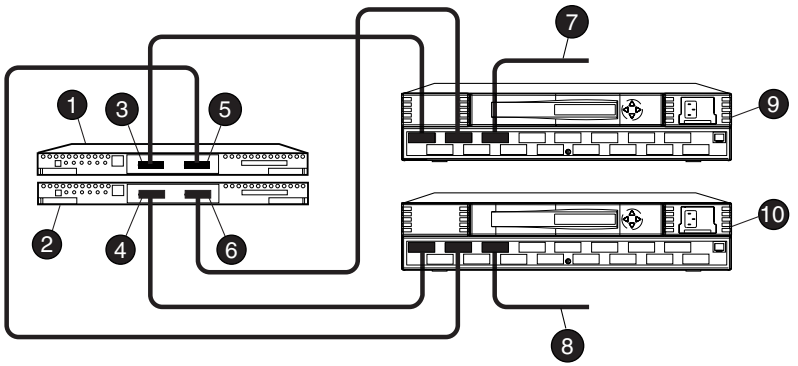

Figure 3: Cabling two RAID controllers and two SAN switches

❶ Top Controller

❷ Bottom Controller

❸ Top Controller, port 1 (to host via top switch)

❹ Bottom Controller, port 1 (to host via bottom switch)

❺ Top Controller, port 2 (to host via bottom switch)

❻ Bottom Controller, port 2 (to host via top switch)

❼ FC cable to host bus adapter A

❽ FC cable to host bus adapter B

❾ SAN Switch (top)

❿ SAN Switch (bottom)

Installing Secure Path Software

3

This chapter describes how to install a new Secure Path software configuration. If you are upgrading an existing Secure Path installation, refer to "Removing/Upgrading Secure Path" on page 119.

This chapter contains the following information that is required for proper Secure Path installation and operation.

Secure Path v3.0D Installation Process Changes

Several significant installation changes have been made in Secure Path v3.0D. The most important change is that parts of the platform kit have been integrated into this kit so that the install requires only Secure Path v3.0D and *does not require a separate platform kit*. The changes are as follows:

- When you uncompress and un-tar the bundle or inspect the CD, the top level, `solaris` directory contains the `install_SP` script. This script is run to *both newly install and upgrade* all valid versions of HBA drivers and Secure Path. Answer **yes** to all queries to remove and replace all currently installed drivers.
- The `/opt/HPfcraid` directory is now used for all newly installed platform components.

Note: The `/opt/HPfcraid` does not replace an installed `/opt/CPQhsv` or `/opt/CPQfcraid` directory. An upgrade to Secure Path 3.0D will not affect any of the old applications *(SSSU* or *SWCC)* in those directories or change their paths.

- The `config.sh` script is included in the `/opt/HPfcraid/bin` directory. This script can be used for adding new arrays or HBAs and HBA ports after the initial install configuration. The procedure to add a new EVA is included in Appendix A.
- The `SSSU` and `SWCC` installation is *not* part of this kit.
- To remove the platform and Secure Path packages, search for all installed packages using `pkginfo | egrep "CPQ|QLA|fca|HP"` and `pkgrm` all found packages.

Installation prerequisites

Note: Before attempting to install Secure Path software, read the Release Notes. The release notes may contain information not found in this installation and reference guide.

Before installing Secure Path v3.0D, verify the following requirements:

- The prerequisites listed under "Operating System Support" in the *HP StorageWorks Secure Path v3.0D Release Notes* have been met.
- The procedures in "Hardware Setup" on page 33 have been performed.
- At least one unit is configured on the RAID storage system and is visible to the server from at least two paths. Ideally, and strongly recommended, the RAID storage systems should be configured with all the desired storagesets/units.

Software installation procedure

Install Secure Path software by performing the following procedures:

Caution: For each RAID system in a production environment that is being converted to Secure Path operation, make sure that all users have logged off the Sun servers and that **all** I/O to the RAID systems has ceased. Follow normal procedures to back up the storage systems before proceeding.

1. Back up the entire system.
2. Check that `vold`, the volume management daemon, is running by entering the following command:

   ```
   # ps -ea | grep vold
   ```

   - If `vold` is currently running:
     a. Insert the Secure Path v3.0D CD-ROM into the CD-ROM drive.
     b. Check that the volume manager has automatically mounted the CD-ROM, by entering the following command:

        ```
        # mount
        ```

Note: The system command may take a few seconds to mount the CD-ROM. If the `mount` command does not indicate that the CD-ROM has been mounted, wait a short interval and then repeat the command. The *volcheck* command can be used to force *vold* to check for mounted media.

c. Change to the Solaris directory by entering the following command:

```
# cd /cdrom/sp_v30d_sun/solaris
```

d. Go to step 3.

- If `vold` is not currently running:

a. Insert the Secure Path v3.0D CD-ROM into the CD-ROM drive.

b. Mount the CD-ROM. For example, enter:

```
# mount -f hsfs -r /dev/dsk/c0t6d0s2 /cdrom
```

c. Change to the Solaris directory by entering:

```
# cd /cdrom/solaris
```

3. Install the Solaris platform software, HBA drivers, and Secure Path by entering the following command:

```
# ./install_SP
```

Answer **yes** to all queries to remove and replace all currently installed drivers.

Note: If Solaris 8 Patch 111097-12/13 or Solaris 9 Patch 113042-04/05 is installed before Secure Path, the Sun native Qlogic driver (qlc) binds to HP FCA2257x (Qlogic) HBAs. If this condition exists, the installation process detects the incorrect binding, requests that you reboot the server after installing the HBA driver but before completing installation, and it requests that you restart the `install_SP` script following reboot. The extra reboot resolves the incorrect binding and allows the installation to complete successfully.

4. Choose from one of the following options:

- If you are configuring only Enterprise Virtual Arrays go to step 6.

- If you are configuring RA8000/EMA12000 arrays, verify critical array settings, set the connection operating system to SUN, set the desired SCSI mode, and record the WWPNs for the array before proceeding:
  a. Using the serial port connection to one of the HSG80 controllers, establish a CLI session to the array.
  b. Verify that the array is in multibus failover mode and in Fibre Channel fabric mode by entering the `show this` and `show other` commands and verifying that the following lines appear for both controllers:

```
Configured for MULTIBUS_FAILOVER with ZG10507050
            In dual-redundant configuration
PORT_1_TOPOLOGY  = FABRIC (fabric up)
PORT_2_TOPOLOGY  = FABRIC (fabric up)
```

  Also verify that at least one unit (LUN) is available to the host by entering the `show units full` command. *At least one LUN must be presented to the host for each array before running `spconfig`.*

  c. Enter the `show connections` command to see the connection settings.

```
CLI> show connections
Connection                                                    Unit
Name      Operating system Controller Port Address  Status   Offset
!NEWCON00   WINNT            THIS      1    1C1100   OL this     0
     HOST_ID=1000-00E0-69C0-0E4D    ADAPTER_ID=2000-00E0-69C0-0E4D
!NEWCON01   WINNT            OTHER     1    1C1100   OL other    0
     HOST_ID=1000-00E0-69C0-0E4D    ADAPTER_ID=2000-00E0-69C0-0E4D
!NEWCON02   WINNT            OTHER     2    671600   OL other    0
     HOST_ID=2000-00E0-8B03-0FB1    ADAPTER_ID=2100-00E0-8B03-0FB1
!NEWCON03   WINNT            THIS      2    671600   OL this     0
     HOST_ID=2000-00E0-8B03-0FB1   ADAPTER_ID=2100-00E0-8B03-0FB1
```

  d. Enter the following commands to set the operating system for each connection name listed:

```
CLI> set !NEWCON00 operating_system = sun
CLI> set !NEWCON01 operating_system = sun
CLI> set !NEWCON02 operating_system = sun
CLI> set !NEWCON03 operating_system = sun
```

Verify your changed settings using the `show connections` command.

e. HP recommends that you set the HSG80 to SCSI-3 mode to make the default SCSI-3 CCL available for all in-band SCSI communications with the array. To set the array to SCSI-3 mode, run the following commands:

```
CLI> set this scsi_version = scsi-3
CLI> restart other
CLI> restart this
```

f. Enter the `show this` and `show other` commands and record the WWPNs for the array. These are listed as `Reported PORT_ID = <WWPN>` and can be used to verify the array being configured in step 5.

Note: If the array is to be shared by other servers connected to the fabric, now would be a good time to set up Selective Storage Presentation. Use the `rename` command to change connection names to unique server/connection identifiers. For example: srv1_con1, srv1_con2, . . .].

`Set Dn disable_access_path=all` and `set Dn enable_access_path=(srv1_con1, srv1_con2...].)` to enable access to that server only. Refer to your HSG80 documentation for more detail.

---

5. Choose from one of the following options:

- If you are configuring RA8000/EMA12000 arrays in SCSI-3 CCL mode, go to step 6.
- If you are configuring RA8000/EMA12000 arrays in SCSI-2 mode, you must complete the following steps to map WWPNs to targets before proceeding:

Note: You can add a CCL in SCSI-2 mode to Secure Path control by using the `spmgr add` command.

---

a. Run the `config.sh` utility. The following example displays both the command line and the Adapter Configuration Menu output:

```
#  /opt/HPfcraid/bin/config.sh


        --- Adapter Configuration Menu ---
              (sd.conf & *fc*.conf)


     1) View Adapters
     2) Add an Adapter or WWPN
     3) Remove an Adapter
     4) Modify an Adapter
     5) View available WWPNs
     q) Exit


Enter choice:
```

b. Select **4) Modify an Adapter** to map the WWPNs to targets. Compare the listed WWPNs to those recorded in step 4, substep c. If array WWPNs are listed for arrays not wanted in the configuration, use the procedure in Appendix A, step 2, Modify Adapter Configuration on page 140, to deselect the unwanted ports. If all ports seen are expected and wanted, proceed to step 5, substep c.

c. Exit `config.sh` by entering a **return** in option **4) Modify an Adapter** and entering **q** in the Adapter Configuration Menu.

d. Reboot the server with a reconfiguration boot. Use the following commands:

```
# touch /reconfigure
# reboot
```

e. Go to step 6 if you need to configure EVA storage. Otherwise continue with step 7.

6. Complete the following steps to allow Secure Path to see the virtual disks (LUNs) of the array if you are configuring Enterprise Virtual Arrays. This procedure assumes you have initialized the storage system and created a disk group.

Refer to the online help system for Command View EVA for detailed information on this procedure.

a. Log onto the Command View Storage Management Appliance from a supported web browser to access the Enterprise Virtual Array storage system.

b. Add the host to the storage system. Before the host can use the storage system's virtual disks, the host must be known to the storage system. Adding the host creates a path from the storage system to *one* host adapter. You must have the host name, host IP address, and HBA World Wide Names to complete this step.

   The HBAs World Wide Names can be obtained by one of the following methods:

   —Run `/opt/HPfcraid/bin/config.sh`, choose Option **5) View available WWPNs** and record the `Adapter ID` numbers.

   —Log into the fabric switch and record the port addresses for the ports attached to the host HBAs.

   —Use the **Add a Host** Element Manager page and the drop down **Port WW Name:** list. This method is unambiguous only if your host is the only new host on the fabric.

Note: On the **Add a Host** page, set the **Host OS:** to `Sun Solaris`.

---

c. Add ports to all remaining host adapters. From the **Host Properties > Ports** page, click **Add port** to add connections to the remaining HBAs.

d. Create and present virtual disks to the host. Follow the steps for Creating a Virtual Disk Family to create the virtual disk family, create virtual disks and present the disks to the host. *At least 1 LUN must be presented to the host for each array before running spconfig*.

   Several options are available for selecting a path preference and mode for a virtual disk. To optimize load balancing, the load should be evenly distributed between controller A and controller B. The boot default selected controller may be chosen by setting the controller *Preferred path/mode*. It is recommended that either *Path A - Failover only* or *Path B*

- *Failover only* be used. This mode allows Secure Path to control failback to the original controller following either a controller failure & replacement or a host reboot.

Note: **Path A - Failover/failback** and **Path B - Failover/failback** are not supported on Secure Path for Solaris.

---

7. Run `spconfig` to configure Secure Path. Refer to the "Configuring the system for Secure Path with spconfig" on page 52 for details on `spconfig` and it's options. `Spconfig` options are required if the host and array are in a SAN with other arrays.
8. Reboot the server with a reconfiguration boot. Use the following commands:

```
# touch /reconfigure
# reboot
```

Configuring the system for Secure Path with spconfig

While installing Secure Path, the software specifically requests that the configuration tool, `spconfig`, be invoked to configure Secure Path.

The `spconfig` tool is a configuration tool for the files `hsx.conf`, `swsp.conf`, `fca-pci.conf`, `fcaw.conf`, `qla2200.conf`, `qla2300.conf` and `sd.conf` that are located in `/kernel/drv`.

The `spconfig` tool requires at least one LUN with at least two visible paths on the server. This LUN allows `spconfig` to communicate with the RAID storage system to gather information required for the previously mentioned configuration files.

The `spconfig` utility is normally run without any options, as follows:

```
#/opt/CPQswsp/bin/spconfig
```

Some configurations may present too many combinations for `spconfig` to determine the desired HBA and RAID storage system combinations. If this is the case, run the `spconfig` utility interactively. This requires user input to define the configuration. Invoke interactive configuration by entering `spconfig` with the *`-o`* switch to indicate operator intervention as shown in the following sample command:

```
# /opt/CPQswsp/bin/spconfig -o
```

Caution: For each RAID system in a production environment being converted to Secure Path operation, make sure that all users have logged off the Sun Solaris servers and that **all** I/O to the RAID systems has ceased. Follow normal procedures to back up the storage systems before proceeding.

Sample spconfig sessions

This section provides two sample sessions: one that is relatively simple, containing no options, and another that is more complex, using the *`-o`* option.

spconfig session without options

The `spconfig` utility configures all visible HP storage arrays, HBAs, and paths for use with Secure Path and generates the configuration files `hsx.conf` and `swsp.conf`. If you are running Solaris 2.6, it also modifies and adds entries to `ssd.conf`.

The following example shows an `spconfig` session running without any options:

```
# /opt/CPQswsp/bin/spconfig
Indicator Key:
.       Inquiry
+   Show This CLI command
-       Show Other CLI command
~   Show Connections CLI command
,       Show Units CLI command
.+-~,.............
Writing conf files.
* * * * * * * *
Done.
#
#
```

Note: If a configuration error was encountered during installation, refer to the next section "Responding to a Configuration Error."

At this point, `spconfig` has completed the necessary file creation and modifications and the system is ready for a configuration.

1. Reboot by entering the following commands:

   ```
   # touch /reconfigure
   # reboot
   ```

2. Verify the Secure Path configuration, after the system has been rebooted, by running the Secure Path Maintenance Tool, `spmgr` as shown in the following example:

   ```
   # spmgr display
   ```

```
Server:  pluto        Report Created: Tue, Oct 02 15:37:36 2001
  Command: ./spmgr display
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  Storage:  5000-1FE1-0010-5D90
  Load Balance: Off  Auto-restore: Off
  Path Verify: On    Verify Interval: 30
  HBAs: fcaw-0  fcaw-1
  Controller:  ZG10505157, Operational
               ZG10505033, Operational
  Devices:  c4t0d0 c4t0d1 c4t0d2 c4t0d3 c4t0d4 c4t0d5
```

```
TGT/LUN   Device          WWLUN_ID          Parent              #_Paths
  0/  0   c4t0d0          6000-1FE1-0010-5D90-0009-1050-5157-0019   4
                                                  /swsp@0,1
       Controller  Path_Instance    HBA            Preferred?  Path_Status
        ZG10505157                                    no
                    hsx-214-33-0     fcaw-0          no           Standby
                    hsx-624-33-0     fcaw-1          no           Standby

       Controller  Path_Instance    HBA            Preferred?  Path_Status
        ZG10505033                                    no
                   hsx-419-32-0     fcaw-0          no           Active
                   hsx-829-32-0     fcaw-1          no          Available
```

spconfig session with options

The following sample procedure shows a partial `spconfig` session with operator intervention. The example is for a system that has a pair of Sbus adapters and a pair of PCI adapters connected to two separate RAID systems.

```
# /opt/CPQswsp/bin/spconfig -o
```

1. `Spconfig` identifies the device, HBA, and RAID storage system and queries if this should be a Secure Path device/target. Answer `yes` or `no` in response to each query. With a yes response, `spconfig` will configure the RAID storage system.

```
-------------------------------------
Found the following target:
   Device:    c3t0d1s0
   HBA:          qla2300-0
   RAID Array: 5000-1FE1-0000-4920
-------------------------------------
Is this a valid SecurePath Device/Target? [y or n]:y
```

2. As `spconfig` displays other devices such as HBAs, and RAID storage system entries, respond with a `yes` or `no` to indicate whether this entry should be part of the Secure Path configuration.

```
-------------------------------------
Found the following target:
   Device:       c4t0d1s0
   HBA:           fcaw0
   RAID Array: 5000-1FE1-0000-5920
-------------------------------------
Is this a valid SecurePath Device/Target? [y or n]:y
```

3. After the Secure Path HBAs and storage systems have been configured, `spconfig` generates the configuration files, `hsx.conf` and `swsp.conf`. If you are running Solaris 2.6, it also modifies and adds entries to `ssd.conf`.

```
Writing conf files.
* * * * * * * *
Done.
#
```

Note: If a configuration error was encountered during installation, refer to the next section "Responding to a Configuration Error."

4. At this point, `spconfig` has completed the necessary file creation and modifications and the system is ready for a configuration reboot by entering the following commands:

```
# touch /reconfigure
# reboot
```

5. After the system has been rebooted, verify the Secure Path configuration by running the Secure Path Maintenance Tool, `spmgr` as shown in the following example:

```
   # spmgr display
Server:  pluto        Report Created: Tue, Oct 02 15:37:36 2001
  Command: ./spmgr display
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  Storage:  5000-1FE1-0010-5D90
  Load Balance: Off  Auto-restore: Off
  Path Verify: On    Verify Interval: 30
  HBAs: fcaw-0  fcaw-1
  Controller:  ZG10505157, Operational
               ZG10505033, Operational
  Devices:  c4t0d0 c4t0d1 c4t0d2 c4t0d3 c4t0d4 c4t0d5

  TGT/LUN   Device           WWLUN_ID           Parent               #_Paths
    0/  0   c4t0d0           6000-1FE1-0010-5D90-0009-1050-5157-0019   4
                                                /swsp@0,1
         Controller  Path_Instance    HBA            Preferred?  Path_Status
          ZG10505157                                    no
                      hsx-214-33-0     fcaw-0          no           Standby
                      hsx-624-33-0     fcaw-1          no           Standby

         Controller  Path_Instance    HBA            Preferred?  Path_Status
          ZG10505033                                    no
                      hsx-419-32-0     fcaw-0          no           Active
                      hsx-829-32-0     fcaw-1         no          Available
```

Logging utility for spconfig

Secure Path v3.0D for Sun Solaris offers a `spconfig` logging utility. When you run `spconfig`, a log file is written to the `/var/adm` directory in the form of `spconfig.<time_stamp>.log`.

The `spconfig` log contains the same output as the `spconfig -v` (verbose) option.

Resolving unconfigured LUN display with spconfig

During installation, `spconfig` configures *all* storage that can be seen from the host. If you do not want all available arrays and/or LUNs configured on the host, use the following steps:

1. Use Selective Storage Presentation to ensure that only desired HBAs have access to LUNs on the storage.
2. Use the `spconfig -o` option when running `spconfig`. This option allows the user to choose what storage is configured under Secure Path control

Stopping I/O during spconfig with an HSG80

If you are using an HSG80 in the configuration, make sure that all I/O to the RAID storage systems being configured is stopped before running `spconfig`. If I/O is running, `spconfig` can fail during the configuration process. If this occurs, make sure all I/O is stopped and rerun `spconfig`.

Selective Storage Presentation with spconfig

HP recommends the use of Selective Storage Presentation (SSP) in a Secure Path environment. SSP is documented in the HSG80 Array Controller CLI Reference Guides. In a Storage Area Network (SAN) environment, use SSP to minimize the chances of data corruption by restricting which Host Bus Adapters (HBAs) have access to certain LUNs on the array at the RAID controller level.

There are also instances when the `spconfig` utility can configure HBAs that may not have been intended for use in the Secure Path environment when SSP is not used. This can only happen when less than the total number of HBAs installed in a host are to be used in the Secure Path configuration. Specifically, if a physical path exists between an HBA and a port on the array that is being used by Secure Path, the LUNs on the array have access set to *all*, and the HBA not intended for Secure Path has the HBA driver loaded; then the HBA can be configured into the Secure Path environment. This is avoided with the proper use of SSP on the storage array.

Responding to configuration errors

Table 5 contains the most probable errors that the Secure Path configuration tool, `spconfig`, reports if it cannot access the current configuration or if it cannot create configuration files for the Secure Path v3.0D installation.

If an error occurs:

1. Take the recommended corrective action to clear the reported problem.
2. Invoke `spconfig` again and verify the problem no longer exists.
3. You may also need to rerun `spconfig` with different options (most likely -o).

Refer to "spconfig command syntax and options" on page 60 for a description of `spconfig` syntax and options.

Spconfig error messages

Table 5: Spconfig errors

Error Message	Description	Corrective action
Invalid argument: *arg*	See usage	See Table 6 on page 60.
directoryArg is not a directory	Argument supplied with -p is not a directory	Make sure the directory supplied with the –p option is a directory.
directoryArg: No such file or directory	No such file or directory for argument supplied with -p	Make sure the directory supplied with the –p option is a directory.
stat(*directoryArg*): *systemError*	Stat error for argument supplied with -p	See stat(2) man page.
alloc(*#bytes*) *systemError*	Out of system memory	Make sure the system has adequate free memory and that it is tuned to allow a single process to access an adequate amount of the free memory.
calloc(): *systemError*	Out of system memory	Make sure the system has adequate free memory and that it is tuned to allow a single process to access an adequate amount of the free memory.
Can't find WWPN for adapter parent *"parent"* type *type*	Could not find the WWPN to match the HBA	Make sure the HBA driver version is supported or that /var/adm/messages contains the WWPN for this adapter.
NULL start of list *arrayPtr HBAPtr*	No valid devices to configure.	Make sure you are in Multiple-bus mode and that your Selective Storage Presentation is correct.

Table 5: Spconfig errors (Continued)

Error Message	Description	Corrective action
NULL start of list on conn *ConnHBAPtr ConnPortPtr*	No valid connections in HSG connection table	Make sure that the connection table contains valid connection data for this host.
Missing D# token	Bad CLI data, could not find D#	Stop all I/O to the storage and rerun *spconfig*.
Corrupt D#	Bad CLI data, the D# is not a number	Stop all I/O to the storage and rerun *spconfig*.
Missing LUN ID: token	Bad CLI data, could not find "LUN ID:" token	Stop all I/O to the storage and rerun *spconfig*.
Missing LUN ID	Bad CLI data, could not find LUN ID	Stop all I/O to the storage and rerun *spconfig*.
Missing Access: token	Bad CLI data, could not find "Access:" token	Stop all I/O to the storage and rerun *spconfig*.
ScsiRecvDiag:Sense key: *key*, ASC: *asc*, ASCQ: *ascq*	CLI error on receive diagnostics	Call support.
ScsiRecvDiag(): devfd=*fileDesc* SendStat=*status* Sense key: *key*, ASC: *asc*, ASCQ: *ascq*	CLI error on receive diagnostics	Verify that monitoring utilities are disable and rerun *spconfig*.

spconfig command syntax and options

The `spconfig` utility is used for configuring during Secure Path installation. This utility generates entries for all HSG devices that are configured for multiple-bus mode. This utility may be run more than once, however it is typically used only for initial system configuration.

Syntax:

```
spconfig
      [-h]
      [-i]
      [-s]
      [-o]
      [-p path]
      [-d number]
      [-v]
```

Table 6 describes the spconfig options.

Table 6: Spconfig options

Option	Description
-h	Displays usage statement.
-i	Disables progress indicators.
-s	Silences all screen output, except errors.
-o	Operator intervention; prompts for each storage system found and asks if you want to add it to the configuration.
-p	Writes configuration files to directory specified by <path>, however prototype and existing files are still read from /kernel/drv.
-d	Modifies dynamic LUN options, where <number> is the number of extra entries to add. The number of entries can be between 0 and 255. The default number of entries (if the -d option is not specified) is 199.
-v	Verbose output, useful for troubleshooting.

Configuration files added or modified by Secure Path v3.0D

Table 7 lists the files added or modified as part of the Secure Path v3.0D installation

Table 7: Configuration files added or modified by Secure Path v3.0D

Files	Description
/kernel/drv/hsx.conf	Configuration file for the hsx driver.
/kernel/drv/swsp.conf	Configuration file for the swsp driver.
/etc/driver_classes	Registers the swsp driver.
etc/devlink.tab	Defines devlinks entry for the swsp driver.
/kernel/drv/fcaw.conf (JNI Sbus driver) /kernel/drv/fca-pci.conf (JNI PCI driver) /kernel/drv/qla2200.conf (Qlogic Sbus, cPCI driver) /kernel/drv/qla2300.conf (Qlogic PCI driver)	Assigns a target number to a controller's World Wide Port Name (WWPN)
/kernel/drv/ssd.conf	Adds pseudo/swsp entries for Secure Path targets on Solaris 2.6 servers.

File format

The following sections list parameters added to files as part of the Secure Path v3.0D installation. Check these files to ensure that the parameters are associated with the appropriate file.

/etc/driver_classes

For the `swsp` driver to be properly associated with a driver class, the installation process adds to the `driver_classes` file:

```
swsp scsi
```

/etc/devlink.tab

So that the Secure Path utilities can communicate with the drivers, the installation process adds to the `devlink.tab` file:

```
type=ddi_pseudo;name=swsp;minor=ctl    swsppCtl
```

/kernel/drv/fcaw.conf (Sbus driver)
/kernel/drv/fca-pci.conf (PCI driver)

In a fabric configuration, a target must be assigned to a WWPN. Target values must be in the range of 32 up to 125, inclusive. For example, to assign target 32 to the port number 5000-1FE1-0000-0D43, `fcaw.conf` would have the following entry:

```
target32_wwpn="50001FE100000D43";
```

/kernel/drv/qla2200.conf (Sbus, cPCI driver)
/kernel/drv/qla2300.conf (PCI driver)

In a fabric configuration, a target must be assigned to a WWPN. Target values must be in the range of 32 up to 255, inclusive. For example, to assign target 32 to the port number 5000-1FE1-0000-0D43, `qla2200.conf` would have the following entry:

```
hba0-SCSI-target-id-32-fibre-channel-port-name="5000IFE100000043";
```

/kernel/drv/hsx.conf

Secure Path device paths are configured by the hsx driver using the entries in the `hsx.conf` file. The entries designate the hardware path, the target assigned to the controller port, and the LUN assignment.

Sample entries in the `hsx.conf` file for the Sbus adapter:

```
name="hsx" parent="/sbus@49,0/fcaw@1,0" target=32 LUN=20
qdepth=32;

name="hsx" parent="/sbus@50,0/fcaw@1,0" target=33 LUN=20
qdepth=32;
```

The target assigned to the controller port is the target number assigned to the port number in the `fcaw.conf` or `fca-pci.conf` file.

Sample entries in the `hsx.conf` file for the PCI adapter:

```
name="hsx" parent="/pci@b,2000/fibre-channel@2" target=32 lun=0
qdepth=32;

name="hsx" parent="/pci@f,2000/fibre-channel@2" target=33 lun=0
qdepth=32;
```

/kernel/drv/swsp.conf

Secure Path device files are configured by the swsp driver using the `swsp.conf` file. Subsequently, the first entry assigns a driver (`swsp`) with a pseudo hardware path for a SCSI class.

```
name="swsp" class="root" portid=0 reg=0x0,0x1,0x1 instance=0
array-name="5000-1FE1-0001-ED10";
```

The other entries in the `swsp.conf` file designate the specific units identified by the World Wide LUN ID assigned by the RAID storage system. For every pair of LUN assignments in `hsx.conf`, there is a matching wwlid_**I**I**T**T**L**L**=**in `swsp.conf`.

- The instance number **I** assigns the LUN to a particular RAID system.
- The target and LUN number **T** and **L** assigns the target and LUN number presented to the SCSI disk driver.

The value assigned must have a corresponding entry in the `/kernel/drv/sd.conf` file. Sample entries in `swsp.conf` file are as follows:

```
wwlid_I0T0L0="6000-1FE1-0001-ED10-0009-9281-0311-0001";
wwlid_I0T0L1="6000-1FE1-0001-ED10-0009-9281-0311-0002";
```

/kernel/drv/ssd.conf

All Secure Path devices on Solaris 2.6 must have a corresponding ssd target entry. Secure Path creates its own `ssd.conf` entries, one per unique target LUN nexus. These entries are placed at the head of the ssd.conf file and allow Secure Path devices to configure prior to other ssd targets. When Secure Path places the `pseudo/swsp.conf` entries at the head of the `ssd.conf` file, conflicts between Secure Path entries and other SCSI bindings are prevented.

Secure Path entries have the format:

```
name=”ssd” parent=”swsp” target=T LUN=L;
```

T represents the target and **L** the LUN number.

For example, Secure Path device target 0 and LUN 0 would have the following entry:

```
name="ssd" parent=”swsp” target=0 LUN=0;
```

Editing files in /etc/CPQswsp

Secure path modifies files contained in the `/etc/CPQswsp` directory. The file `spmgr_stop_list` can be edited to add to the list of reserved words that `spmgr alias` will not use to create aliases. The other two files in the directory, `notify.ini` and `spmgr_alias`, must not be edited. They are text files, but are used exclusively by Secure Path.

Secure Path and the CCL

Secure Path provides support for both SCSI-2 and SCSI-3 CCL modes. During the installation of Secure Path, a special driver (cpqccl) is loaded that allows Solaris to recognize the SCSI-3 CCL. For simplicity, this is the preferred mode. You can also configure the CCL in SCSI-2 mode. In this case, the system sees the CCL as a read-only disk.

Using SCSI-3 with the CCL

Secure Path v3.0D for Sun Solaris provides the `cpqccl` driver for SCSI-3 CCL mode. This is the only mode that the Enterprise Virtual Array supports. The HSG80 controllers can also support this mode—refer to the ACS Reference Guide for instructions on setting the CCL mode to SCSI-3. With SCSI-3 CCL mode enabled, `spconfig` automatically maps WWPNs for all storage that can be accessed during Secure Path installation.

Using SCSI-2 with the CCL

Manually mapping WWPNs with SCSI-2

When you enable SCSI-2 or SCSI-2 CCL mode, the WWPN mappings must be done manually using `config.sh`, and the system rebooted, before you can run `spconfig`. Refer to step 5 in the "Software installation procedure" in this chapter on page 48 to manually map WWPNs.

Adding CCLs in SCSI-2 mode

You can add a CCL in SCSI-2 mode to Secure Path control by using the `spmgr add` command. The SCSI-2 CCL must be configured with the Solution Software (platform kit), and must be visible to the system with the format command before it can be added.

Managing Secure Path

4

This chapter describes the user interface for the Secure Path v3.0D Management utility `spmgr`. It includes the following topics:

Note: Examples are based on the HSG80 controller, but all actions are identical for the HSV110/HSV100 controllers.

Secure Path Manager overview

The Secure Path Manager (spmgr) utility lets you monitor and manage devices, storage systems, and paths to units that are in the Secure Path configuration. It also lets you modify the configuration to repair, replace, or reconfigure. The spmgr utility relies on spagent to handle calls to the driver (swsp).

Spmgr commands

Table 8 lists the spmgr commands options. Their format and usage are presented and described in the sections following the tables.

Table 8: Spmgr commands

Command	Options/arguments	Description
spmgr add	WWLUNID [target [LUN]] -r WWNN all	Add a new device to the Secure Path configuration.
spmgr alias	alias_name old_name no argument	Assign an alias to an object.
spmgr client	add remote_host_name delete remote_host_name	Adds or deletes a remote spmgr client host
spmgr delete	WWLUNID device -r WWNN all	Removes a device from the Secure Path configuration.
spmgr display	-a[v] [adapter] -c[v] [controller_ser_num] -d[v] [device] -p path-Instance -r[v] [WWNN] -u -l no argument	Displays information about configured Secure Path devices.
spmgr log	-c 0, 1...3 -l 0, 1...3 -n 0, 3 no argument	Sets logging to the console, system log file, and e-mail notification.

Table 8: Spmgr commands (Continued)

Command	Options/arguments	Description
spmgr notify	add severity_level email_address delete email_address no argument	Manage e-mail address and event logging severity to each e-mail recipient.
spmgr password | passwd	new_password	Sets the spagent password required for remote client access.
spmgr quiesce	-a adapter -c controller_ser_num -p path_instance	Move I/O to an alternative object and temporarily remove selected object from use.
spmgr restart	-a adapter -c controller_ser_num -p path_instance all	Return a previously quiesced object to an active or available state.
spmgr remote_host_name:*spmgr_command*	spmgr commands alias, notify, client, password and display -l are not supported	Executes an spmgr command on a remote host.
spmgr restore	-d device -r WWNN all	Restore one or more devices to their preferred I/O path.
spmgr select	-c controller_ser_num [-d device[-f]] -p path_instance [-f]	Select and prefer a path for I/O.

Table 8: Spmgr commands (Continued)

Command	Options/arguments	Description
spmgr set	-a on | off [WWNN] (-a auto restore) -b on | off [WWNN] (-b load balancing) -b rr [WWNN] (rr round robin (default) on) -b ls [WWNN] (ls least service time on) -b li [WWNN] (li least I/O outstanding on) -b lb [WWNN] (lb least bandwidth on) -p on | off [WWNN] (-p path verification) -f interval (1 to 65535 seconds)	Enable or disable special driver functionality.
spmgr unalias	alias_name old_name	Delete an alias.
spmgr update		Updates *swsp.conf* with the driver's current state

Note: Commands typed without an argument respond with "usage" if the command is a configuration altering command. The commands—*alias, display, log,* and *notify*—respond with current command or configuration information.

Spmgr common terms

Table 9 describes the common `spmgr` terms. For a more complete list of Secure Path terms, refer to the Glossary on page 155.

Table 9: Spmgr common terms

Term	Definition
Device	The standard representation for a device or device link on a server. For example: c*X*t*Y*d*Z*.
Logical Unit	A device that is managed by Secure Path and identified by its 32-digit World Wide LUN Identifier (WWLUNID).
Adapter	The operating system ID of the HBA.
Storage System Array WWNN	A storage system is identified by its 16-digit World Wide Node Name (WWNN).
Controller serial number	The controller is identified by a unique serial number. The serial number of the HSG80 is a 10-character alphanumeric string.

Displaying configuration information

Controller states

Table 10 lists the controller states and their descriptions.

Table 10: Controller states

Controller States	Description
Failed	This state may mean a failed or offline condition because the server cannot communicate with the other controller at this time.
Operational	The controller is available with a good status.
Unknown	The server cannot communicate with this controller.

Path states and attribute

Table 11 lists and describes the path states reported by the Secure Path driver.

Table 11: Path states and attribute

Path States/Attribute	Description
Active	This state indicates that the path is currently used for the I/O stream or is available for load balancing.
Available	This state indicates that the path is available on the active controller for the I/O stream.
Failed	This state indicates that the path is currently unusable for the I/O stream.
Quiesced	This state indicates that the path may be valid, but has been made unavailable for I/O.
Standby	This state indicates that the path is valid on the standby controller.
Preferred	This attribute indicates that the path is preferred for the I/O stream, across reboots. It may not be assigned to either a failed or a quiesced path.

Device states

Table 12 lists and describes device states.

Table 12: Device states

Device states	description
Critical	Only one path remains available to the storage unit.
Degraded	At least one or more paths are failed to the storage unit.
Operational	All paths are available to the storage unit.
Unknown	Unable to communicate with the unit. This may indicate no available path or a failed device.
Failed	Paths are available but an inquiry to the device returns a not-ready state even after retries.

Display header information

Due to the possible complexity of the Secure Path configuration and the possibility of shared storage or clustered software across multiple servers, the display information always has two standard lines of information at the start of the display:

```
Line 1: Server: Server Name    Report Created: Date and Time
Line 2: Command: Command string
```

Display differences between HSG and HSV controllers

All general examples in this document use the HSG80 serialization format and actual HSG80 examples. The HSG80 and HSV110/HSV100 Array Controllers present objects to Secure Path in identical ways, therefore there are no differences in the way you manage settings, paths, and devices using the `spmgr` management utility.

There are however, two differences in serialization of Array objects that allow you to quickly determine which type of array is being displayed. The following examples list the differences:

```
HSG80

Controller Serial Number ZG10506981

Array World Wide Node Name (WWNN) 5000-1FE1-0010-5B00

World Wide LUN ID (WWLUNID)
6000-1FE1-0010-5B00-0009-1050-6981-1234


HSV110/HSV100

Controller Serial Number P4889B29LC01J

Array World Wide Node Name (WWNN) 5000-1FE1-0015-0AE0

World Wide LUN ID (WWLUNID)
6005-08B4-0001-40BF-0000-A000-1234-0000
```

Note: The location of the sequence "1234" in the WWLUNID examples is unique for each LUN and is in a different position for the array types.

The display Command

This section describes the spmgr display commands and associated switch parameters. Each switch results in a different type of display.

Note: The verbose flag may only be used with some, but not all, cases of the command.

Syntax:

```
# spmgr display -a[v] [adapter]
            -c[v] [controller_ser_num]
            -d[v] [device]
            -p path_instance
            -r[v] [WWNN]
            -l
            -u
            (no argument)
```

For each of these command switches, this section presents:

- Description
- Syntax
- All forms of the command
- Examples of all forms of the command
- Example displays of all forms of the command

spmgr display

When you enter `spmgr display`, all information for the entire configuration is displayed. The amount of information displayed depends on the number of HBAs, storage systems, and paths to a unit on each storage system.

The full display derives from the component portions described in this section. You can limit the amount of data displayed by combining the `spmgr display` command with one of the described switches.

Example:

```
   # spmgr display
Server:  pluto        Report Created: Tue, Oct 02 15:37:36 2001
Command: ./spmgr display
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5000-1FE1-0010-5D90
Load Balance: Off  Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: fcaw-0  fcaw-1
Controller:  ZG10505157, Operational
             ZG10505033, Operational
Devices:  c4t0d0 c4t0d1 c4t0d2 c4t0d3 c4t0d4 c4t0d5
```

```
  TGT/LUN   Device           WWLUN_ID           Parent               #_Paths
    0/  0   c4t0d0           6000-1FE1-0010-5D90-0009-1050-5157-0019   4
                                                /swsp@0,1
          Controller  Path_Instance    HBA            Preferred?  Path_Status
           ZG10505157                                    no
                       hsx-214-33-0     fcaw-0          no           Standby
                       hsx-624-33-0     fcaw-1          no           Standby

          Controller  Path_Instance    HBA            Preferred?  Path_Status
           ZG10505033                                    no
                       hsx-419-32-0     fcaw-0          no           Active
                       hsx-829-32-0     fcaw-1         no          Available


TGT/LUN   Device           WWLUN_ID           Parent               #_Paths
    0/  1   c4t0d1           6000-1FE1-0010-5D90-0009-1050-5157-001A   4
                                                /swsp@0,1
          Controller  Path_Instance    HBA            Preferred?  Path_Status
           ZG10505157                                    no
                       hsx-215-33-1     fcaw-0          no           Standby
                       hsx-625-33-1     fcaw-1          no           Standby

          Controller  Path_Instance    HBA            Preferred?  Path_Status
           ZG10505033                                    no
                       hsx-420-32-1     fcaw-0          no           Active
                       hsx-830-32-1     fcaw-1         no          Available


  TGT/LUN   Device           WWLUN_ID           Parent               #_Paths
    0/  2   c4t0d2           6000-1FE1-0010-5D90-0009-1050-5157-001B   4
                                                /swsp@0,1
          Controller  Path_Instance    HBA            Preferred?  Path_Status
           ZG10505157                                    no
                       hsx-216-33-2     fcaw-0          no           Standby
                       hsx-626-33-2     fcaw-1          no           Standby

          Controller  Path_Instance    HBA            Preferred?  Path_Status
           ZG10505033                                    no
                       hsx-421-32-2     fcaw-0          no           Active
                       hsx-831-32-2     fcaw-1         no          Available
```

spmgr display -a[v] [HBA]

The -a switch lists HBA (host bus adapter) related information. If a parameter is supplied, it must be the *adapter instance number*.

Syntax:

```
# spmgr display -a
          -av
          -a HBA
          -av HBA
```

When the -a switch is used without a parameter, the display contains a complete list of all HBAs in the Secure Path configuration from the server where the command is entered.

Example:

```
# spmgr display -a
  Server:  pluto    Report Created: Fri, Mar 05 12:28:27 2004
  Command: spmgr display -a
  Adapters in the Secure Path Configuration
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
    qla2300-0,   qla2300-1
```

When the -a switch is paired with the v switch, the display contains a list of all adapters in the Secure Path configuration. In this case, the v acts like a wildcard for the device switch, -a.

Example:

```
# spmgr display -av
  Server:  pluto    Report Created: Fri, Mar 05 12:28:44 2004
  Command: spmgr display -av
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  Adapter:       qla2300-0
  Parent:        /pci@8,700000/QLGC,qla@2
  Manufacturer:  QLogic Corporation
  Version:       v.4.13.01
  Firmware:      v.3.2.15 IP
  Optional ROM:  v.QLogic QLA2300 Fibre Channel Host Adapter
fcode version 1.18.3 12/03/01


  Adapter:       qla2300-1
  Parent:        /pci@8,700000/QLGC,qla@3
  Manufacturer:  QLogic Corporation
  Version:       v.4.13.01
  Firmware:      v.3.2.15 IP
  Optional ROM:  v.QLogic QLA2300 Fibre Channel Host Adapter
fcode version 1.18.3 12/03/01
```

When invoked with the -a switch and HBA, the display shows the Solaris path attached to the HBA, as shown in the following example:

Example:

```
# spmgr display -a qla2300-0
  Server:  pluto    Report Created: Fri, Mar 05 12:29:02 2004
  Command: spmgr display -a qla2300-0
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  Adapter:       qla2300-0
  Parent:        /pci@8,700000/QLGC,qla@2
  Manufacturer:  QLogic Corporation
  Version:       v.4.13.01
  Firmware:      v.3.2.15 IP
  Optional ROM:  v.QLogic QLA2300 Fibre Channel Host Adapter
fcode version 1.18.3 12/03/01
```

When invoked with the -a switch, v switch, and HBA, the display shows all paths attached to the HBA, as shown in the following example:

Example:

```
# spmgr display -av qla2300-0
  Server:  pluto    Report Created: Fri, Mar 05 12:33:14 2004
  Command: spmgr display -av qla2300-0
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  Adapter:       qla2300-0
  Parent:        /pci@8,700000/QLGC,qla@2
  Manufacturer:  QLogic Corporation
  Version:       v.4.13.01
  Firmware:      v.3.2.15 IP
  Optional ROM:  v.QLogic QLA2300 Fibre Channel Host Adapter
fcode version 1.18.3 12/03/01


  Storage:  5000-1FE1-5000-38A0
  Item  Device       Controller     HBA                    Instance
  = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  0   c3t0d0      P4889B59IM5049 qla2300-0    /swsp@0,1    hsx-0-40-1
       WWPN: 50001FE1500038AC     Path State: Standby
  1   c3t0d0      P4889B49IM401J qla2300-0    /swsp@0,1    hsx-208-39-1
       WWPN: 50001FE1500038A9     Path State: Active [P]
```

spmgr display -c[v] [controller_serial_number]

The -c switch displays controller related information. If a parameter is supplied, it must be a *controller_serial_number*. The command has four possible forms:

Syntax:

```
# spmgr display -c
                -cv
                -c controller_serial_number
                -cv controller_serial_number
```

Example:

```
# spmgr display -c
Server:  pluto        Report Created: Tue, Oct 02 14:51:50 2001
Command: ./spmgr display -c
Current Controller List
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
ZG10505157, ZG10505033
```

Example:

```
# spmgr display -cv
Server:  pluto        Report Created: Tue, Oct 02 14:51:55 2001
Command: ./spmgr display -cv
Controller: ZG10505157  Status: Operational
Vendor: Compaq
WWNN: 5000-1FE1-0010-5D90
WWPN1: 5000-1FE1-0010-5D93
HBAs: fcaw-0, fcaw-1

Controller: ZG10505033  Status: Operational
Vendor: Compaq
WWNN: 5000-1FE1-0010-5D90
WWPN1: 5000-1FE1-0010-5D91
HBAs: fcaw-0, fcaw-1
```

Example:

```
# spmgr display -c ZG10505167
Server:  pluto        Report Created: Tue, Oct 02 14:52:35 2001
Command: ./spmgr display -c ZG10505157
Controller: ZG10505157  Status: Operational
Vendor: Compaq
WWNN: 5000-1FE1-0010-5D90
WWPN1: 5000-1FE1-0010-5D93
HBAs: fcaw-0, fcaw-1
```

Example:

```
# spmgr display -cv ZG10505167

Server:  pluto        Report Created: Tue, Oct 02 14:52:53 2001
Command: ./spmgr display -cv ZG10505157
Controller: ZG10505157  Status: Operational
Vendor: Compaq
WWNN: 5000-1FE1-0010-5D90
WWPN1: 5000-1FE1-0010-5D93
HBAs: fcaw-0, fcaw-1

Item  Device   Controller   HBA        Parent          Instance
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
0     c4t0d0  ZG10505157   fcaw-0  /swsp@0,1         hsx-214-33-0
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
1     c4t0d0  ZG10505157   fcaw-1  /swsp@0,1         hsx-624-33-0
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
2     c4t0d1  ZG10505157   fcaw-0  /swsp@0,1         hsx-215-33-1
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
3     c4t0d1  ZG10505157   fcaw-1  /swsp@0,1         hsx-625-33-1
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
4     c4t0d2  ZG10505157   fcaw-0  /swsp@0,1         hsx-216-33-2
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
5     c4t0d2  ZG10505157   fcaw-1  /swsp@0,1         hsx-626-33-2
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
6     c4t0d3  ZG10505157   fcaw-0  /swsp@0,1         hsx-217-33-3
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
7     c4t0d3  ZG10505157   fcaw-1  /swsp@0,1         hsx-627-33-3
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
8     c4t0d4  ZG10505157   fcaw-0  /swsp@0,1         hsx-218-33-4
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
9     c4t0d4  ZG10505157   fcaw-1  /swsp@0,1         hsx-628-33-4
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
10    c4t0d5  ZG10505157   fcaw-0  /swsp@0,1         hsx-219-33-5
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
11    c4t0d5  ZG10505157   fcaw-1  /swsp@0,1         hsx-629-33-5
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
```

spmgr display –d[v] [device]

The -d switch displays device related information. If a parameter is supplied, it must be a *device*.

Syntax:

```
# spmgr display –d
                -dv
                -d   [device]
                -dv  [device]
```

Example:

```
# spmgr display -d
Server:  pluto        Report Created: Tue, Oct 02 14:54:05 2001
Command: ./spmgr display -d
Devices by Storage System
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5000-1FE1-0010-5D90

   Devices:  c4t0d0  c4t0d1  c4t0d2  c4t0d3  c4t0d4  c4t0d5
```

Example:

```
# spmgr display -dv
Server:  Pluto     Report Created: Mon, Jan 13 15:48:24 2003
Command: spmgr display –dv
Device:       c6t0d7
Status:       Operational  [4 paths (1/0/2)]
Storage:      5000-1FE1-0016-6C30
LUNID:        6000-1FE1-0016-6C30-0009-2030-2549-0026
Preferred Controller: None
HBAs:  qla2300-0 qla2300-1

Device:       c6t0d8
Status:       Operational  [4 paths (1/0/2)]
Storage:      5000-1FE1-0016-6C30
LUNID:        6000-1FE1-0016-6C30-0009-2030-2549-0027
Preferred Controller: None
Grouped LUNs: c6t0d8  c6t0d9  c6t0d10
HBAs:  qla2300-0 qla2300-1
```

```
Device:       c6t0d9
Status:       Operational  [4 paths (1/0/2)]
Storage:      5000-1FE1-0016-6C30
LUNID:        6000-1FE1-0016-6C30-0009-2030-2549-0028
Preferred Controller: None
Grouped LUNs: c6t0d8  c6t0d9  c6t0d10
HBAs:  qla2300-0 qla2300-1

Device:       c6t0d10
Status:       Operational  [4 paths (1/0/2)]
Storage:      5000-1FE1-0016-6C30
LUNID:        6000-1FE1-0016-6C30-0009-2030-2549-0029
Preferred Controller: None
Grouped LUNs: c6t0d8  c6t0d9  c6t0d10
HBAs:  qla2300-0 qla2300-1
```

Note: Secure Path displays path states using the following convention:
[total number of paths (active/failed/standby)]
Actual numerical equivalents replace the text.
For example, the following attributes are displayed as [10 paths (8/0/2)]:
Total paths = 10, Active = 8, Failed = 0, Standby = 2

Example:

```
# spmgr display -d c6t0d7
  Server:  Pluto     Report Created: Mon, Jan 13 15:41:27 2003
  Command: spmgr display -d c6t0d9
  Device:       c6t0d9
  Status:       Operational  [4 paths (1/0/2)]
  Storage:      5000-1FE1-0016-6C30
  LUNID:        6000-1FE1-0016-6C30-0009-2030-2549-0028
  Preferred Controller: None
  Grouped LUNs: c6t0d8  c6t0d9  c6t0d10
  HBAs:  qla2300-0  qla2300-1
```

Example:

```
# spmgr display -dv c6t0d9
  Server:  Pluto     Report Created: Mon, Jan 13 15:47:19 2003
  Command: spmgr display -dv c6t0d9
  Device:       c6t0d9
  Status:       Operational  [4 paths (1/0/2)]
  Storage:      5000-1FE1-0016-6C30
  LUNID:        6000-1FE1-0016-6C30-0009-2030-2549-0028
  Preferred Controller: None
  Grouped LUNs: c6t0d8  c6t0d9  c6t0d10
  HBAs:  qla2300-0  qla2300-1
 Item  Device       Controller     HBA          Parent Instance
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
  0   c6t0d9       ZG20400420     qla2300-0    /swsp@0,2 hsx-2535-37-11
        WWPN: 5000-1FE1-0016-6C32  Path State: Active
  1   c6t0d9       ZG20302549     qla2300-0    /swsp@0,2 hsx-2773-38-11
        WWPN: 5000-1FE1-0016-6C33  Path State: Standby
  2   c6t0d9       ZG20400420     qla2300-1    /swsp@0,2 hsx-3027-36-11
        WWPN: 5000-1FE1-0016-6C31  Path State: Available
  3   c6t0d9       ZG20302549     qla2300-1    /swsp@0,2 hsx-3265-39-11
        WWPN: 5000-1FE1-0016-6C34  Path State: Standby
```

spmgr display –p path_instance

The -p switch displays storage path information. A parameter is required and it must be a *path_instance*.

Syntax:

```
# spmgr display -p path_instance
```

Example:

```
# spmgr display –p hsx-219-33-5
  Server:  pluto        Report Created: Tue, Oct 02 14:58:32 2001
  Command: ./spmgr display -p hsx-219-33-5
  Path:      hsx-219-33-5              Adapter: fcaw-0
  Controller: ZG10505157                  Status:  Operational
  Device:     c4t0d5                      Status:  Operational
```

spmgr display –r[v] [WWNN]

The -r switch displays storage system information. If a parameter is supplied, it must be a *WWNN*. The command has the following possible forms:

Syntax:

```
# spmgr display  -r
                 -rv
                 -r WWNN
                 -rv WWNN
```

Example:

```
# spmgr display -r
Server:  pluto        Report Created: Tue, Oct 02 14:59:39 2001
Command: ./spmgr display -r
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5000-1FE1-0010-5D90
```

Example:

```
# spmgr display -rv
Server:  pluto        Report Created: Tue, Oct 02 14:59:49 2001
Command: ./spmgr display -rv
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5000-1FE1-0010-5D90
Load Balance: Off  Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: fcaw-0  fcaw-1
Controller:  ZG10505157, Operational
             ZG10505033, Operational
Devices:  c4t0d0 c4t0d1 c4t0d2 c4t0d3 c4t0d4 c4t0d5
```

Example:

```
# spmgr display -r 5000-1FE1-0010-5D90
Server:  pluto        Report Created: Tue, Oct 02 15:02:34 2001
Command: ./spmgr display -r 5000-1FE1-0010-5D90
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5000-1FE1-0010-5D90
Load Balance: Off  Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: fcaw-0  fcaw-1
Controller:  ZG10505157, Operational
             ZG10505033, Operational
Devices:  c4t0d0 c4t0d1 c4t0d2 c4t0d3 c4t0d4 c4t0d5
```

Example:

```
# spmgr display -rv 5000-1FE1-0010-5D90
Server:  pluto        Report Created: Tue, Oct 02 15:02:51 2001
Command: ./spmgr display -rv 5000-1FE1-0010-5D90
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5000-1FE1-0010-5D90
Load Balance: Off  Auto-restore: Off
Path Verify: On    Verify Interval: 30
HBAs: fcaw-0  fcaw-1
Controller:  ZG10505157, Operational
             ZG10505033, Operational
Devices:  c4t0d0 c4t0d1 c4t0d2 c4t0d3 c4t0d4 c4t0d5
Path Information: [P] = Preferred

Item  Device   Controller   HBA      Parent           Instance
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
0     c4t0d0  ZG10505157   fcaw-0  /swsp@0,1         hsx-214-33-0
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
1     c4t0d0  ZG10505033   fcaw-0  /swsp@0,1         hsx-419-32-0
      WWNN: 5000-1FE1-0010-5D90      Path State: Active
2     c4t0d0  ZG10505157   fcaw-1  /swsp@0,1         hsx-624-33-0
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
3     c4t0d0  ZG10505033   fcaw-1  /swsp@0,1         hsx-829-32-0
      WWNN: 5000-1FE1-0010-5D90      Path State: Available
4     c4t0d1  ZG10505157   fcaw-0  /swsp@0,1         hsx-215-33-1
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
5     c4t0d1  ZG10505033   fcaw-0  /swsp@0,1         hsx-420-32-1
      WWNN: 5000-1FE1-0010-5D90      Path State: Active
6     c4t0d1  ZG10505157   fcaw-1  /swsp@0,1         hsx-625-33-1
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
7     c4t0d1  ZG10505033   fcaw-1  /swsp@0,1         hsx-830-32-1
      WWNN: 5000-1FE1-0010-5D90      Path State: Available
8     c4t0d2  ZG10505157   fcaw-0  /swsp@0,1         hsx-216-33-2
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
9     c4t0d2  ZG10505033   fcaw-0  /swsp@0,1         hsx-421-32-2
      WWNN: 5000-1FE1-0010-5D90      Path State: Active
10     c4t0d2  ZG10505157   fcaw-1  /swsp@0,1         hsx-626-33-2
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
11     c4t0d2  ZG10505033   fcaw-1  /swsp@0,1         hsx-831-32-2
      WWNN: 5000-1FE1-0010-5D90      Path State: Available
12     c4t0d3  ZG10505157   fcaw-0  /swsp@0,1         hsx-217-33-3
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
13     c4t0d3  ZG10505033   fcaw-0  /swsp@0,1         hsx-422-32-3
      WWNN: 5000-1FE1-0010-5D90      Path State: Active
14     c4t0d3  ZG10505157   fcaw-1  /swsp@0,1         hsx-627-33-3
```

```
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
15     c4t0d3  ZG10505033   fcaw-1  /swsp@0,1        hsx-832-32-3
      WWNN: 5000-1FE1-0010-5D90      Path State: Available
16     c4t0d4  ZG10505157   fcaw-0  /swsp@0,1        hsx-218-33-4
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
17     c4t0d4  ZG10505033   fcaw-0  /swsp@0,1        hsx-423-32-4
      WWNN: 5000-1FE1-0010-5D90      Path State: Active
18     c4t0d4  ZG10505157   fcaw-1  /swsp@0,1        hsx-628-33-4
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
19     c4t0d4  ZG10505033   fcaw-1  /swsp@0,1        hsx-833-32-4
      WWNN: 5000-1FE1-0010-5D90      Path State: Available
20     c4t0d5  ZG10505157   fcaw-0  /swsp@0,1        hsx-219-33-5
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
21     c4t0d5  ZG10505033   fcaw-0  /swsp@0,1        hsx-424-32-5
      WWNN: 5000-1FE1-0010-5D90      Path State: Active
22     c4t0d5  ZG10505157   fcaw-1  /swsp@0,1        hsx-629-33-5
      WWNN: 5000-1FE1-0010-5D90      Path State: Standby
23     c4t0d5  ZG10505033   fcaw-1  /swsp@0,1        hsx-834-32-5
      WWNN: 5000-1FE1-0010-5D90      Path State: Available
```

spmgr display -u

This command requires no parameter and returns a display of all unattached units for each storage system. This switch provides the list of units by storage system and reports the WWLUN ID for each. The information gathered by this display may then be used to add a unit to the Secure Path configuration.

Example:

```
  # spmgr display  -u
Server:  pluto        Report Created: Tue, Oct 02 15:52:56 2001
Command: ./spmgr display -u
Storage:  5000-1FE1-0010-5D90
LUN ID:   6000-1FE1-0010-5D90-0009-1050-5157-0020
          6000-1FE1-0010-5D90-0009-1050-5157-0021
```

spmgr display -l

This command requires no parameter and returns a display of all unused target/LUNs for each storage system. This switch provides a list of units by storage system, and displays the device file for each. The information gathered from this display may be used to add a unit to the Secure Path configuration at a particular target/LUN.

Example:

```
  # spmgr display -l
Server:  pluto    Report Created: Thu, Oct 11 09:30:13 2001
Command: ./spmgr display -l
Available Target/Luns per Storage System
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
Storage:  5000-1FE1-0005-B5F0
c4t0d5, c4t0d6, c4t0d7, c4t0d8, c4t0d9, c4t0d10, c4t0d11, c4t0d12, c4t0d13
c4t0d14, c4t0d15, c4t0d16, c4t0d17, c4t0d18, c4t0d19, c4t0d20, c4t0d21,
c4t0d22, c4t0d23, c4t0d24, c4t0d25, c4t0d26, c4t0d27, c4t0d28, c4t0d29,
c4t0d30, c4t0d31, c4t0d32, c4t0d33, c4t0d34, c4t0d35, c4t0d36, c4t0d37,
c4t0d38, c4t0d39, c4t0d40, c4t0d41, c4t0d42, c4t0d43, c4t0d44, c4t0d45,
c4t0d46, c4t0d47, c4t0d48, c4t0d49, c4t0d50, c4t0d51, c4t0d52, c4t0d53,
c4t0d54, c4t0d55, c4t0d56, c4t0d57, c4t0d58, c4t0d59, c4t0d60, c4t0d61,
c4t0d62, c4t0d63, c4t0d64, c4t0d65, c4t0d66, c4t0d67, c4t0d68, c4t0d69,
c4t0d70, c4t0d71, c4t0d72, c4t0d73, c4t0d74, c4t0d75, c4t0d76, c4t0d77,
c4t0d78, c4t0d79, c4t0d80, c4t0d81, c4t0d82, c4t0d83, c4t0d84, c4t0d85,
c4t0d86, c4t0d87, c4t0d88, c4t0d89, c4t0d90, c4t0d91, c4t0d92, c4t0d93,
c4t0d94, c4t0d95, c4t0d96, c4t0d97, c4t0d98, c4t0d99, c4t0d100, c4t0d101,
c4t0d102, c4t0d103, c4t0d104, c4t0d105, c4t0d106, c4t0d107, c4t0d108,
c4t0d109, c4t0d110, c4t0d111, c4t0d112, c4t0d113, c4t0d114, c4t0d115,
c4t0d116, c4t0d117, c4t0d118, c4t0d119, c4t0d120, c4t0d121, c4t0d122,
c4t0d123, c4t0d124, c4t0d125, c4t0d126, c4t0d127, c4t0d128, c4t0d129,
c4t0d130, c4t0d131, c4t0d132, c4t0d133, c4t0d134, c4t0d135, c4t0d136,
c4t0d137, c4t0d138, c4t0d139, c4t0d140, c4t0d141, c4t0d142, c4t0d143,
c4t0d144, c4t0d145, c4t0d146, c4t0d147, c4t0d148, c4t0d149, c4t0d150,
c4t0d151, c4t0d152, c4t0d153, c4t0d154, c4t0d155, c4t0d156, c4t0d157,
c4t0d158, c4t0d159, c4t0d160, c4t0d161, c4t0d162, c4t0d163, c4t0d164,
c4t0d165, c4t0d166, c4t0d167, c4t0d168, c4t0d169, c4t0d170, c4t0d171,
c4t0d172, c4t0d173, c4t0d174, c4t0d175, c4t0d176, c4t0d177, c4t0d178,
c4t0d179, c4t0d180, c4t0d181, c4t0d182, c4t0d183, c4t0d184, c4t0d185,
c4t0d186, c4t0d187, c4t0d188, c4t0d189, c4t0d190, c4t0d191, c4t0d192,
c4t0d193, c4t0d194, c4t0d195, c4t0d196, c4t0d197, c4t0d198, c4t0d199,
c4t0d200, c4t0d201, c4t0d202, c4t1d0, c4t2d0, c4t3d0, c4t4d0, c4t5d0,
c4t6d0, c4t8d0, c4t9d0, c4t10d0, c4t11d0, c4t12d0, c4t13d0, c4t14d0,
c4t15d0
```

The alias and unalias commands

Secure Path supports the use of aliases. Aliases replace or substitute longer strings for shorter strings.

Alias supports the ISO 8859 character set (characters 33 to 176) excluding colons or embedded spaces and supports alias names up to 16 characters in length. Aliases may not be defined or referenced using `spmgr remote` commands. Only one alias per object is allowed. The following Secure Path `spmgr display` objects may be aliased:

- Storage (WWNN)
- HBA
- Controller
- Device
- WWLUN_ID
- Controller
- Path_Instance
- WWPN

Example:

The World Wide Node Name (WWNN) of a storage system is `5000-1FE1-0005-3480`. You can assign the alias *Bird* to replace the longer, less easy-to-remember WWNN `5000-1FE1-0005-3480`.

When an alias is used in an `spmgr display` command, it is shown in parenthesis after the term that it substitutes for.

Example:

Storage: 5000-1FE1- 0001-3420 (fire)

The alias is fire.

Alias commands:

- Define an alias and store it for future use.
- Remove an alias from the alias table.
- Display the alias table.

spmgr alias alias_name old_name

To add an alias to the alias table use the following alias command.

Syntax:

```
# spmgr alias alias_name old_name
```

The following example creates the alias *Birdtop* for the controller serial number: ZG66654211.

```
# spmgr alias Birdtop ZG66654211
```

spmgr unalias

To remove an alias from the alias table invoke the `spmgr unalias` command and enter either the *alias_name* or the *old_name*.

Syntax:

```
# spmgr unalias  old_name
                     alias_name
```

In the following example, the alias, *Birdtop*, is removed from the alias table.

```
# spmgr unalias Birdtop
```

spmgr alias

Use the alias command to display the alias table.

Syntax:

```
# spmgr alias
```

Example:

```
# spmgr alias
Server:  Pluto Report Created: Wed, Aug 15 15:42:37 2001
Alias:old_string
= = = = = = = = = = = = = =
bob:5000-1fe1-0000-1231
jim:5000-1fe1-0000-1233
fredt:ZG111298235442
fredb:ZG238817633215
= = = = = = = = = =  = =  = =
```

Note:

- When the `spmgr display` command is invoked, the screen output uses both the alias, if any, and the standard Storage system WWNN or controller serial number. The alias will be enclosed in parentheses (alias_name).
- For a command set that requires a parameter, it is assumed that the parameter or its alias may be input. Commands cannot be aliased.

The `spmgr alias` command is used to reference a large cumbersome old_name with a shorter or clearer alias_name. Reversing the argument order such as `spmgr alias old_name alias_name` results in the `alias_name` replacing the `old_name` so that any command using the `old_name` results in error. The alias must then be deleted for the `old_name` to again work correctly.

The `spmgr alias` command checks a table of reserved words to protect you from aliasing words that would result in unexpected behavior. However, this list is not comprehensive. Take precautions to avoid using special characters such as a leading "-" or "$", that could be misinterpreted by the shell.

The current list of reserved words maintained by `spmgr` is:

add all alias client delete display help

log notify on off password prefer quiesce restart

restart restore select set spmgr unalias unprefer

update version

Setting storage system parameters

The Secure Path v3.0D driver has options you can enable or disable on a storage system or global basis. These options may be turned off and on dynamically. These changes occur within 45 seconds.

- The `spmgr set` command lets you enable storage system specific settings for the Secure Path driver.
  - **Load balancing**–v3.0D of Secure Path implements one of four load balancing algorithms that use all available paths to a unit for its I/O. The default for load balancing is disabled. If load balancing is enabled, the default algorithm is Round Robin.
  - **Path verification**–The driver checks the state of all possible paths to all units at a settable period or frequency. The default for path verification is enabled with a period of 30 seconds.
  - **Auto-restore**–The auto-restore command enables the driver to automatically restore paths to their preferred path after a failure and subsequent reinstatement of that path. The default for Auto-restore is disabled.
- The `spmgr log` command lets you enable logging from the Secure Path driver to the syslog, console and e-mail notification.
- The `spmgr notify` command lets you manage the distribution of the three classes of event reports (critical, warning and informational) via an e-mail address list.

The set command

Syntax:

```
# spmgr set -a (on | off) [WWNN]
            -b (on | off) [WWNN]
             -b rr [WWNN]
             -b ls [WWNN]
             -b li [WWNN]
             -b lb [WWNN]
             -p (on | off) [WWNN]
             -f verify_period
```

spmgr set -a on | off [WWNN]

This command enables or disables the Auto-Restore feature of the driver. When Auto-Restore is enabled, it directs the driver to monitor the state of the paths. If the preferred path should fail and then later return to service, the driver will automatically reroute all I/O to the restored path. When Auto-Restore is disabled, there is no Auto-Restore by the Secure Path driver. The I/O will continue along the current paths until another event changes the active path. On initial Secure Path installation the default for Auto-Restore is **off**.

Note: If you enable Auto-Restore using `spmgr set -a on` and select a new path using `spmgr select <path>`, the selected path will not stay selected and will be auto-restored. This behavior is different from that of Secure Path on the HP-UX platform.

If this "toggling" continues, it will trigger the anti-thrash filter. This filter prevents Auto-restore from operating for approximately one hour. When the anti-thrash filter is enabled, you will see the following message in your system message file:

```
CPQswsp: Auto restore for LUN WWLUNID has been disabled
until next time quantum (1 hour)
```

---

spmgr set -b on | off [WWNN]

This command enables or disables the load balancing option of the driver. When load balancing is enabled, all available paths on the Active controller are marked as Active and I/O is sent to the unit along all Available paths using the default Round Robin algorithm. When load balancing is disabled, the I/O will be sent along the Preferred Path (if one is selected) or will use the first available path for I/O. On initial Secure Path installation, the default for load balancing is **off**.

spmgr set -b rr [WWNN]

This command enables Round Robin load balancing. The Round Robin algorithm rotates through all available paths on the active controller with equal distribution to each.

If load balancing is disabled, this command will enable Round Robin. If load balancing is enabled, this command will change the balancing algorithm to Round Robin. If the WWNN argument is provided, load balancing is enabled for just that array. Otherwise, the command applies to all configured arrays.

spmgr set -b ls [WWNN]

This command enables Least Service Time load balancing. The Least Service Time algorithm uses the available path on the active controller that has the least outstanding I/O bytes count.

If load balancing is disabled, this command will enable Least Service Time. If load balancing is enabled, this command will change the balancing algorithm to Least Service Time. If the WWNN argument is provided, load balancing is enabled for just that array. Otherwise, the command applies to all configured arrays.

spmgr set -b li [WWNN]

This command enables Least I/O load balancing. The Least I/O algorithm uses the available path on the active controller that has the least outstanding I/O requests.

If load balancing is disabled, this command will enable Least I/O. If load balancing is enabled, this command will change the balancing algorithm to Least I/O. If the WWNN argument is provided, load balancing is enabled for just that array. Otherwise, the command applies to all configured arrays.

spmgr set -b lb [WWNN]

This command enables Least Bandwidth load balancing. The Least Bandwidth algorithm uses the available path on the active controller which takes the least average time to complete a command.

If load balancing is disabled, this command will enable Least Bandwidth. If load balancing is enabled, this command will change the balancing algorithm to Least Bandwidth. If the WWNN argument is provided, load balancing is enabled for just that array. Otherwise, the command applies to all configured arrays.

spmgr set -p on | off [WWNN]

This command enables or disables the path verification of the driver. When enabled, this command verifies the state of all possible paths to all units. On large configurations with active I/O to many units, this command may reduce performance. On initial Secure Path installation, the default for path verification is **on**.

spmgr set -f (1…65535 seconds)

This command sets the path verification interval. This interval can be set between 1 to 65535 seconds. The use of the -f switch does not change the current state of the path verification, it will only change the value for the interval. Therefore, if path verification is disabled, it remains disabled with the new interval. On initial Secure Path installation, the default path verification interval is set to 30 seconds.

The log command

Syntax:

```
# spmgr log -l (level  0, 1..3)
            -c (level  0, 1..3)
            -n (level  0, 3)
```

The numerical level indicates the message severity. The levels of severity are:

1: Critical, 2: Warning, 3: Informational

When you select a numerical level, messages of that severity and higher are delivered to the appropriate output.

- If 3 is selected, then 3,2,1 are logged
- If 2 is selected, then 2,1 are logged
- If 1 is selected, then 1 is logged
- If 0 is selected, then logging is disabled for that item

spmgr log -l [0, 1..3]

This command sets the level of logging to the syslog of the server. When you select level 1…3, the messages of that severity and higher are written to the `syslog` file. The default is 2.

spmgr log -c [0,1..3]

This command sets the level of logging to the console. When you select level 1..3, the messages of that severity and higher are displayed on the console. The default is 1.

spmgr log -n [0, 3]

This command enables or disables logging to the notify function. This option has two values 0, and 3. The default is 3. Level 0 is provided for disabling all notification messages.

spmgr log

The `spmgr log` command displays the current logging settings.

Example:

```
    # spmgr log
Server:  Pluto Report Created: Wed, Aug 15 15:42:37 2001
Current Log Options
= = = = = = = = = = = = = = = = = = = = =
Syslog,enabled,level 2
Console,disabled,level 0
Notify,enabled,level 3
= = = = = = = = = = = = = = = = = = = = =
```

The notify command

The notify command lets you manage the distribution of the three classes of event reports: critical, warning, and informational. In Secure Path v3.0D, notification occurs through e-mail.

Syntax:

```
#spmgr  notify add
                delete
                (no argument)
```

Severity levels

Messages from the Secure Path drivers are one of three severity levels:

- Critical messages are severity level 1.
- Warning messages are severity level 2.
- Informational messages are severity level 3.

Notify sends event notices to users from the highest to the lowest level of the severity marking as follows:

- A user with severity level 3 receives level 3, 2, and 1 severity messages.
- A user with severity level 2 receives level 2 and 1 severity messages.

- A user with severity level 1 receives severity level 1 messages only.

spmgr notify add

This command adds an e-mail address to the notification list.

Syntax:

```
# spmgr notify add severity_level  email_address
```

Example:

```
# spmgr notify add 3 john.doe@oscar.edu.it
```

Severity_level is 3 and the email_address is john.doe@oscar.edu.it

---

Note: A user is defined by a unique email_address. A user with more than one email_address may have multiple records, one for each unique address.

---

spmgr notify delete

This command deletes an e-mail address from the notification list.

Syntax:

```
# spmgr notify delete email_address
```

Example:

```
# spmgr delete julie.smith@hollywood.edu
```

The email_address is julie.smith@hollywood.

spmgr notify

This command displays the list of users to be notified that have been saved in configuration files.

Example:

```
   # spmgr notify
Server: Pluto          Report Created: Wed, Aug 15 15:42:37 2001
Command: spmgr notify
     Current Log Options
Severity      Mode       email_address
= = = = = = = = = = = = =  = =  = = = = = = = = = = = = = = =
1             M          bob.proliant@compaq.com
2             M          evil.knevil@jump.into.the.net
3             M          harry.houdini@magic.org
= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =
```

Path management

Secure Path v3.0D supports up to 32 paths to a unit on a storage system. Given the very large number of paths that can be configured for a single system, `spmgr` provides you with the ability to monitor and manage paths.

The path management actions include:

- Selecting and preferring paths
- Restoring preferred paths
- Quiescing and restarting objects and paths

The select command

A path is a combination of all the components from server to the unit on the storage system. When you describe the entire path you must identify the HBA and the controller port.

Selecting paths means to identify a path to be used for I/O and to Prefer that path. Path information, including Selected and Preferred paths can be viewed with one or more options of the `spmgr display` command.

When paths are selected for I/O they are intended to remain selected during a server reboot or power cycle, and are referred to as *preferred paths*.

Syntax:

```
spmgr select  -c controller_ser_num [-d device [f]]
              -p path_instance [f]
```

Note: The command `spmgr select` *–a HBA [device]* has been removed for v3.0D.

spmgr select -c controller_serial_number

This command selects a path or paths with the indicated controller serial number and makes those paths Active and Preferred. For example, if there are three HBAs with paths through one controller, the Secure Path driver marks one path for each device from one HBA, not necessarily the same HBA. The result is to have identified selected and Preferred paths for multiple units with this command.

Example:

```
# spmgr select –c ZG10505167
```

Result: The Secure Path driver marks each first probed path to each unit, through controller ZG10505167, as the selected and Preferred path for I/O.

spmgr select -c controller_serial_number –d device

This command selects a path with the indicated controller and device and makes that path Active and Preferred. Since a specific path is not specified, the first probed path is selected. This command selects one controller and one device on that controller. Therefore, the driver is able to mark one path for the chosen device on that controller as Selected. The overall result is to have identified selected paths for a single unit with this command.

If the device is part of a group that has its members all active on the other controller, the command will fail with a message: “Warning: LUN is part of a group in which at least one other member is preferred to the other controller. To force action, rerun command with the -f option.”

Example:

```
# spmgr select –c ZG10505167 –d c21t0d2
```

Result: The Secure Path driver marks the first probed path through the controller, ZG10505167 to unit c21t0d2 as the selected and Preferred path for I/O.

spmgr select -c controller_serial_number –d device -f

This command forces the selection of the specified device. If the device is part of a group and the selection moves the device to the other controller, all other devices in the group are moved to the other controller and the first probed path on those devices are marked as Active and Preferred. All other preferences to the devices in the group are removed.

Example:

```
# spmgr select –c ZG10505167 –d c21t0d2 –f
```

Results: The operation is completed and if the LUN is part of a group and the other controller is specified/implied, all other members of the group are moved to that controller and the first probed paths are marked as Active and Preferred.

spmgr select -p path_instance

This command selects the indicated path and makes that path Active and Selected. This parameter, path_instance, contains the necessary components of HBA, controller port, and device. Therefore, no other switches or parameters are required to identify the path.

If the LUN is part of a group and the path_instance is on the other controller, the command will fail with a message: “Warning: LUN is part of a group in which at least one other member is preferred to the other controller. To force action, rerun command with the -f option.”

Example:

```
# spmgr select –p hsx-219-33-5
```

Result: The Secure Path driver marks path hsx-219-33-5 as the selected path for I/O.

spmgr select -p path_instance -f

This command forces the selection of the specified path_instance. If the device associated with the path is part of a group and the selection moves the device to the other controller, all other devices in the group are moved to the other controller. The selected path and the first probed path on all other devices in the group are marked as Active and Preferred. All other preferences to the devices in the group are removed.

Example:

```
# spmgr select –p hsx-219-33-5 –f
```

Results: The operation is completed and if the device associated with the path is part of a group and the selected path is on the other controller, all other members of the group are moved to that controller and the selected path and the first probed path on all other devices in the group are marked as Preferred.

Note: The s`pmgr select` command completion time is dependent on total number of paths involved in the selection. The select command does not return a command prompt until the selection is complete. The time can range from a few seconds for a single path selection to tens of minutes for selecting a controller in a configuration with greater than 50 LUNs. To avoid this delay, HP recommends preferring the controller by setting the preferred controller LUN attribute.

Spmgr select, restore and partitioned storagesets

Using `spmgr select` and `spmgr restore` on LUNs that are part of a partitioned HSG80 storageset results in all LUNs of that partition being selected or restored. If the path being selected is on the opposite controller from the currently active path, the `spmgr select -f -c controller_serial_number` operation (with the `-f` option to force the controller change) causes the HSG80 to move control of the storageset to that controller. All LUNs that are partitions of that storageset will also be moved. If the path being restored is on the opposite controller from the currently active path, the `spmgr restore` operation will NOT move the Active path to the other controller. The `spmgr select` command must be used to move control between controllers.

Preferring paths and group IDs overview

The `spmgr prefer` and `spmgr unprefer` commands have been removed in v3.0D. The `spmgr select` command selects the paths as the Active paths and in v3.0D, prefers the selected paths and marks them Preferred in `spmgr display`.

On an array, each LUN may be assigned or Preferred to a particular controller and be available for selection at startup. This feature is enabled by using the HSG80 or HSV110/HSV100 management utilities.

Because Secure Path can have more than one path to each controller, you can further specify a *preferred path* by selecting that path. To differentiate between the controller unit attribute of Preferred_path and the Secure Path *preferred path,* this document refers to the controller-based Preferred_path attribute as the *preferred controller.*

The preferred path assignment lets you control setting static load balancing because the path chosen determines which adapter and controller port are designated as the default path at system startup. One preferred path can be assigned to each controller for each LUN.

For the Preferred Path feature to work, you must set either the preferred controller LUN attribute on the array or the preferred path attribute on Secure Path, or both the preferred controller and preferred path attributes.

Preferred path identifications are marked by the Secure Path driver in the running system and the identifications are stored in the configuration files for that driver. Therefore, the path may be maintained permanently until another path is selected.

On first boot, the Preferred controller will come up as the Active controller if it has been preferred at the array. If not preferred at the array, the first probed controller comes up as the Active controller. On first boot, the first probed path on the Preferred or first probed controller comes up as the Active path but it is not preferred.

Understanding load balancing and active paths (preferred or selected)

Preferred path and Selected path are meaningless designations when you have enabled load balancing. Load balancing treats all paths equally and directs I/O to all available paths. In other words, load balancing is a higher priority than Preferred or Selected paths.

When load balancing is enabled, the Secure Path driver will attempt to use all the available paths to a LUN using the algorithm you specified with the `spmgr set` command and all paths on the active controller are shown as Active and Preferred in `spmgr display`.

If load balancing is enabled and you select a path on the Active controller, the system performs the following actions:

- The driver marks the path as Preferred but the path will not be used as Preferred until the load balancing is turned off. The path continues to be used as one of the set of active paths.
- The configuration file for paths will have this path marked as preferred and upon reboot this path will be marked as preferred and deployed as preferred if and when load balancing is disabled.

If load balancing is enabled and you select a path on the Standby controller, the system performs the following actions:

- The driver initiates failover to the selected controller, marks the old active controller as the Standby controller, and marks the new controller as the Active controller. The driver marks the selected path as Preferred but the path will not be used as Preferred until the load balancing is turned off. The path continues to be used as one of the set of active paths on the new controller.
- The configuration file for paths will have this path marked as preferred and upon reboot this path will be marked as Preferred and deployed as Preferred if and when load balancing is disabled.

If load balancing is enabled, both paths on the active controller are marked as Active and Preferred. If Auto Restore is also enabled and a controller is Preferred, then failing and repairing a controller results in a restored preferred controller. Preferred controllers have priority over load balancing.

If load balancing and Auto Restore are both enabled and paths on either controller are preferred but no controller is preferred, then failing and repairing paths or controller will not result in an Auto Restore. Load balancing has priority over preferred paths in this case.

Group IDs

HSG80 Devices, Stripsets, and Raidsets may be divided into up to 8 partitions. Partitioned LUNs sharing the same device, Stripset or Raidset are said to be in the same Group and share the same Group ID. All LUNs sharing the same Group ID must follow certain rules in order to prevent undesired behaviors. For example, operations that move a LUN from one controller to the other controller must be applied to all LUNs in the Group. Secure Path v3.0D implements these rules regarding Group IDs and displays Group IDs in `spmgr display -d device`, `spmgr display -dv` and `spmgr display -dv device`.

Examples of Preferred Path Priority

If multiple LUNs share the same Group ID the following applies:

- If a path is selected (`spmgr select -p path`) then that path and all first probed paths on all the other LUNs in the Group are marked as Preferred.
- If the paths of a Group on Controller A are preferred and a path or a device on Controller B is selected (`spmgr select -p path` or `spmgr select -c controller_ser_num -d device`) then the selection will fail with a message:

```
"Warning: LUN is part of a group in which at least one other
member is preferred to the other controller.  To force action,
rerun command with the -f option."
```

- If the paths of a Group on Controller A are preferred and a path or a device on Controller B is selected and forced (`spmgr select -p path -f` or `spmgr select -c controller_ser_num -d device -f`) then that path and all first probed paths on all the other LUNs in the Group are marked as Preferred and all previously preferred paths on Controller A will be cleared in `spmgr display` but remembered as Preferred paths in the driver.
- If the paths of a Group on Controller A are preferred and Controller B is selected (spmgr select `-c controller_ser_num`), then all first probed paths on all the LUNs in the Group on Controller B are marked as Preferred and all previously preferred paths on Controller A will be cleared in `spmgr display` but remembered as Preferred paths in the driver.

If LUNs DO NOT share the same Group ID then the following applies:

- If a path is selected (`spmgr select -p path`) then that path is marked as Preferred.
- If a path on Controller A is preferred and a path or a device on Controller B is selected (`spmgr select -p path` or `spmgr select -c controller_ser_num -d device`) then that path or the first probed path of the device on Controller B is selected and marked as Preferred and the previously preferred path on Controller A is cleared in `spmgr display` but is remembered as a preferred path in the driver.
- If a path or paths on Controller A are preferred and Controller B is selected (`spmgr select -c controller_ser_num`), then all first probed paths on all the LUNs on Controller B are marked as Preferred and the previously preferred path or paths on Controller A are cleared in `spmgr display` but are remembered as a preferred paths in the driver.

Setting the preferred controller LUN attribute

For ease of use, HP recommends setting the preferred controller LUN attribute for all LUNs under Secure Path control.

To set the preferred controller LUN attribute for the HSG80, use the HSG80 ADD or SET commands and the Preferred_path attribute for preferring a unit to *this* or *other* controller. For example, a unit can be assigned to be preferred to *this* controller by entering the following command:

```
HSG80> SET D6 PREFERRED_PATH = THIS_CONTROLLER
```

To set the preferred controller LUN attribute for the HSV110/HSV100, log onto the Command View EVA Manager and execute the following steps for preferring a virtual disk to controller A or controller B:

1. Select the virtual disk you want to modify in the Navigation pane.
2. Set the **Preferred Path/Mode to Path A-Failover Only** or **Path B-Failover Only** on the Virtual Disk Active Properties page.
3. Choose **Save Changes** at the top of the Content pane to direct the system to process the change. A status page displays indicating whether the modification was completed successfully.
4. Click **OK**. An updated Properties page displays.

Assigning grouped LUNs to different servers

Although LUNs that are members of a partitioned group may be assigned to different servers, it is recommended that grouped LUNs under Secure Path control be assigned to the same server. Multiple path failures on one server can cause a controller failover that is not recognized by the other server. In extreme cases, both servers may compete for different controllers, resulting in ping-pong failovers between controllers.

The restore command

The default for `spmgr restore` is to return all LUNs to their preferred path if load balancing is disabled.

By using one or more of the switches for this command, you have full control of restoring preferred paths to the Secure Path configuration.

The use of this command assumes three important conditions:

- Paths were preferred previously. If paths to some LUNs have not been preferred, no action will be performed on those units.
- The restore does not require moving a LUN or LUNs to the other not-preferred controller. A restore will not move units to the other controller unless that is the preferred controller. If the preferred LUN controller attribute is not set and you wish to move controllers, use the `spmgr select` command to accomplish that.
- Load balancing is currently disabled. If load balancing is currently enabled, no action will be performed on any path.

Syntax:

```
spmgr restore all
              -d device
              -r WWNN
```

spmgr restore all

Restores all LUNs to their preferred paths and/or preferred controller. If there is no preferred controller, the default will be the current controller. If there is no preferred path, the default will be the current path.

Syntax:

```
# spmgr restore all
```

Example:

```
# spmgr restore all
```

spmgr restore -d *device*

Restores a preferred path to the indicated device.

Syntax:

```
# spmgr restore -d device
```

Example:

```
# spmgr restore -d c21t0d2
```

If a preferred path to a device is in the failed state and you issue a `spmgr restore -d <device>`, the command line responds with a prompt (no apparent response). The path remains in a failed state and no path change is made. This is the expected response to the command.

spmgr restore -r *WWNN*

Restores a preferred path to the indicated storage system.

Syntax:

```
# spmgr restore -r WWNN
```

Example:

```
# spmgr restore -r 5000-1FE1-0010-5B00
```

The quiesce command

Quiescing an object means to:

- Move all active I/O from an object to an alternate path.
- Mark all paths to the object as *quiesced* to temporarily remove the object from use.

The objects that are supported for v3.0D of Secure Path are adapters and controllers. Also, quiescing individual paths is supported to allow other fabric infrastructure, such as switches, to be removed and replaced.

Note: Path verification is not performed on a quiesced path.

Syntax:

```
# spmgr quiesce  -a HBA
                 -c controller_serial_number
                 -p path_instance
```

spmgr quiesce -a HBA

When this command is invoked, `spmgr` will move all active I/O using this HBA to paths available on other HBAs. The paths of the specified HBA will then be marked as *quiesced* and no further I/O will be sent along that path until the HBA is returned to service with the corresponding restart command.

These actions may be verified by issuing the # spmgr display –a HBA to view the current path state.

Use this feature to move I/O to another adapter as the first step to replacing an HBA.

Example:

```
# spmgr quiesce -a fcaw-0
```

spmgr quiesce -c controller_serial_number

When this command is invoked, `spmgr` moves all active I/O using this controller to paths on the other controller of the storage system. The paths of the specified controller will then be marked as *quiesced* and no further I/O will be sent along that path until the controller is returned to service with the restart command.

These actions may be verified by issuing the # spmgr display –c controller command to view the current path states.

Use this feature to move I/O to the other controller as the first step to upgrading or replacing a controller.

Example:

```
# spmgr quiesce -c ZG11233409
```

spmgr quiesce -p path_instance

When this command is invoked, `spmgr` moves all active I/O using this path to another path on the same controller if possible or to a path on the *other* controller. The specified path will then be marked as *quiesced* and no further I/O will be sent along that path until the path is returned to service with the restart command.

These actions may be verified by issuing the `spmgr display` command to view the current path states.

Example:

```
# spmgr quiesce –p hsx-219-33-5
```

The restart command

Object restarting changes a quiesced adapter or controller to an Available or Standby state. When restarted, the HBA or controller is available as an I/O entity for a path.

Syntax:

```
# spmgr restart all
          -a HBA
          -c controller
          -p path_instance
```

spmgr restart all

When this command is invoked, `spmgr` verifies the existence of all components on quiesced paths and change those paths to Available or Standby as appropriate. If the Auto-restore feature is enabled and one or more of those paths are Preferred paths, those paths will be made the Active path.

spmgr restart -a HBA

When this command is invoked, `spmgr` verifies the existence of the HBA and then change the state of the paths using the HBA to Available or Standby. If the Auto-restore feature is enabled and a path using that HBA is the preferred path, the path will be made the Active path.

Example:

```
# spmgr restart -a fcaw-0
```

spmgr restart -c controller

When invoked, `spmgr` verifies the existence of the controller and then change the state of the paths using the controller to Standby. If the Auto-restore feature is enabled and a path using that controller is the preferred path, then the path will be made the Active path.

Example:

```
# spmgr restart -c fire-top
```

spmgr restart -p path_instance

When invoked, `spmgr` verifies the existence of the path and then change the state of the path to Available or Standby. If the Auto-restore feature is enabled and the path is the preferred path, the path will be made Active.

Example:

```
# spmgr restart –p hsx-219-33-5
```

The add and delete commands

Secure Path v3.0D supports the dynamic addition and removal of LUNS on a storage system. There are several steps required to add and delete LUNs:

1. Create the units on the storage system.
2. Run `drvconfig` so that the system sees the new units.
3. Enter either the `spmgr display -u` command if adding LUNs or the `spmgr display -dv` command if deleting LUNs to obtain the WWLUNID of the units.
4. Enter the `spmgr add` or `spmgr delete` command to add or delete the units.
5. Enter the `drvconfig;disks` command to attach the new units, and create the device files if you are running Solaris 2.6.

The delete command

The `spmgr delete` command prevents you from deleting a LUN that is open or mounted. If you attempt to delete an open LUN, the command fails and the following error message displays:

```
Error: Device mounted or otherwise busy.
```

The add command

The `spmgr add` command prevents you from adding a LUN that contains failed paths. An attempt to add a LUN with failed paths results in the following error message:

```
Error: Invalid Argument.
```

Deleting units

If you are deleting units, these options will not remove the orphaned device files or on Solaris 2.6, format displays deleted devices as `drive type unknown`. Choose the appropriate option below depending on your specific requirements:

- Enter the `devfsadm -C` command (Solaris Version 7, 8, and 9 only) to force Solaris to clean up device links.
- Enter the `reboot -- -r` command on Solaris 2.6 to shut down your server and force a reconfiguration boot.

- Ignore them. The format command will show the disks as *unknown* because there is nothing there to respond to SCSI commands. As long as nothing attempts to access these units, you will not have a problem. This option works well if you are adding and deleting cloned units for backup purposes. You may add and delete new units using the same target and LUN repeatedly.

spmgr add WWLUNID [target LUN]

This command verifies access to the new unit and adds that device to the Secure Path configuration. At the same time, the configuration files are updated.

This command requires administrative commands before and after use. Prior to using `spmgr add`, new units must be found by the system and after the add, units must be claimed by the system. The following command sequence must be done at least once for adding single or multiple units.

Syntax:

```
# spmgr add WWLUNID [target LUN]
```

- `WWLUNID` is the World Wide LUN ID of the new unit you are adding on the storage system.
- `target LUN` (optional) is the target and LUN values to assign for the server

Example:

Note: Remember, create the new unit(s) on the storage system before you run this command.

To probe for and attach to new unit(s):

```
# drvconfig
```

To display unmapped WWLUNID(s):

```
# spmgr display -u
```

To add units:

```
# spmgr add WWLUNID1 [target LUN]
# spmgr add WWLUNID2 [target LUN]
# spmgr add WWLUNIDn [target LUN]
```

To attach new units and create device files on Solaris 2.6 hosts only:

```
# drvconfig; disks
```

spmgr add –r WWNN all

WWNN is the World Wide Node Name of the array that will have all of its units added to the Secure Path configuration.

This command identifies all unclaimed units for the specified array and add them all to the Secure Path configuration. This command can take up to 15 minutes to complete for the maximum (128) number of units.

Note: The new storage arrays cannot be added to your server without rebooting. This is due to the static nature of the HBA drivers. Port/target mappings must be defined and the server rebooted *before* Secure Path can access the new storage.

Syntax:

```
# spmgr add –r WWNN all
```

Example:

```
# spmgr add –r 5000-1FE1-000-1234 all
```

When invoked, the Secure Path driver probes for all unclaimed units associated with the specified Array and if available, add them to the data. At the same time, the configuration files will be updated.

This command can only be used when the HBA drivers are configured to map WWPNs to targets, and at least one LUN is under Secure Path control. In other words, at least one LUN on a storage system must be visible with the `spmgr display` command before you can use the `spmgr add -r WWNN all` command. Create and dynamically add additional LUNS to Secure Path with the `spmgr add -r WWNN all` command.

If you do not have at least one LUN of the array visible to Secure Path, follow the procedures in "Adding an Array to an Existing Configuration" on page 131.

spmgr delete WWLUNID | device

This command verifies the device and if correct, deletes the device from the Secure Path configuration. These actions occur only on the server where the command was issued. For shared storage, the unit must be deleted on each server that has access to it.

Note: Units must be deleted from Secure Path control before they are deleted from the storage or unpresented.

This command requires administrative steps after it is used. These steps are discussed in more detail in "The add and delete commands" on page 110.

Syntax:

```
# spmgr delete WWLUNID | device
```

Example:

```
# spmgr delete fireD12
```

In this example, Alias *fireD12* is used instead of the WWLUNID.

To identify the WWLUNIDs:

```
# spmgr display -dv
```

To delete units:

```
# spmgr delete WWLUNID1
# spmgr delete WWLUNID2
# spmgr delete WWLUNIDn
```

To remove orphaned device files on Solaris 7, 8 and 9 (optional), enter the following command:

```
# devfsadm -C
```

spmgr delete –r WWNN all

This command identifies all unclaimed units for the specified array and deletes them all from the Secure Path configuration. This command can take up to 15 minutes to complete for the maximum (128) number of units.

Syntax:

```
# spmgr delete -r WWNN all
```

WWNN is the World Wide Node Name of the array that will have all of its units deleted from the Secure Path configuration.

Example:

```
# spmgr delete -r 5000-1FE1-000-1234 all
```

This command verifies the array and if correct, will delete all of the array's devices from the configuration.

These actions occur only on the server where the command was issued. For shared storage, the unit must be deleted on each server that has access to it.

After the delete, the following command sequence must be issued at least once to delete the units from the system.

Example:

```
# spmgr display (to identify the WWNN of the Array to be
deleted)

# spmgr delete -r WWNN all
```

To remove orphaned device files on Solaris 7, 8, and 9 (optional), enter the following command:

```
# devfsadm -C
```

Note: Use `devfsadm -C` with Solaris 7, 8 or 9 only. For Solaris 2.6 you must perform a `reboot -- -r` reconfiguration boot.

Remote execution of spmgr

By design, `spmgr` is a network program. The `spmgr` utility communicates the `spagent` daemon via sockets. The `spmgr` can communicate with `spagent` from a remote system.

Remote systems or clients gain access to the Secure Path driver by a `spagent` connection through a password-protected entry. The password is encrypted at the client site and verified against the password stored on the server. Both server and client systems must have Secure Path v3.0D installed.

Clients will petition the `spagent` for access to `spmgr` with the password and their client name. If both the client name and password are correct, the client will be granted access. If either the client name or the password is incorrect, the petitioner will be denied access.

Remote spmgr tasks include:

- Adding or deleting a remote client
- Setting the local password
- Executing a remote spmgr command

spmgr client add remote_host_name

This command instructs `spagent` to validate and store a client system for access to manage the local Secure Path configuration.

Example:

```
# spmgr client add pluto
```

Result: System *pluto* is added as a valid client to send remote Secure Path commands to the local server host.

spmgr client delete remote_host_name

This command instructs `spagent` to delete a client system for access to manage the local Secure Path configuration.

Example:

```
# spmgr client delete pluto
```

Result: System *pluto* is deleted as a valid client and cannot send remote Secure Path commands to the local host.

spmgr password | passwd new_password

The command sets the local password required by client systems for access to manage the local Secure Path configuration.

Example:

```
# spmgr passwd ageB4beauty
```

Result: The local password is changed to *ageB4beauty.*

spmgr remote_host_name:spmgr_command

The command request `spagent` to execute the `spmgr` command `spmgr_command` on the remote client *`remote_host_name`*. If the remote client is listed in the local list of valid clients and the remote client's `spagent` password matched the `spagent` password set on the local host, the command is executed and the results listed to the local host.

The following spmgr commands cannot be executed remotely:

alias

client

display -l

notify

password | passwd

Example:

```
# spmgr mickey:display
```

Result: The spagent daemon sends the command to the server system. The server system validates the client system name in it's client list, validates the client password, execute the remote command and sends the output to the client system where it is displayed.

The update command

The update command updates the `swsp.conf` file with the driver's current state.

Syntax:

```
# spmgr update
```

Removing/Upgrading Secure Path

5

This chapter describes the following information to remove and/or upgrade Secure Path software:

Removing Secure Path software

Removing the Secure Path software restores the server to a single-path, RAID storage environment. Under a single-path configuration, the HSG80 controller must be set into Transparent Failover mode. The steps to accomplish the transition of the HSG80 controllers to Transparent Failover mode are described in Appendix B on page 147.

To remove Secure Path software:

1. On the specific servers, invoke the Sun package remove function and select CPQswsp as shown below:

   ```
   # pkgrm CPQswsp
   ```

2. Go to the directory `opt/HPfcraid/bin`

   ```
   # cd /opt/HPfcraid/bin
   ```

3. Enter the following command:

   ```
   # ./config.sh
   ```

   During Secure Path installation, target entries are removed from the `/kernel/drv/sd.conf` file and moved to the `hsx.conf` and `swsp.conf` files.

   The following steps will regenerate the `sd.conf` file for use with the Fibre Channel drivers as a single-path application. During these steps, new target names and new LUN values may be chosen.

4. Select Option **4) Modify Adapters**.

   a. Select each adapter and reselect:

   — The mode of operation

   — The desired targets

   — The desired number of LUNs

   — The specific WWPNs for the intended RAID storage system.

   b. Choose **Return** to complete each adapter update and the changes will be made to the `/kernel/drv/sd.conf` and to the Fibre Channel driver configuration files, `<hba_type>.conf`.

5. Restart the server. Enter the following:

   ```
   # touch /reconfigure
   # reboot
   ```

Reconfiguring the RAID controllers

If the RAID storage system is to be used for single-path access by one or more servers, then the HSG80 dual-redundant controllers must be restored to Transparent Failover mode.

Refer to "HSG80 Controller Failover Transitions" on page 147 to perform the transition to Transparent Failover mode.

Upgrading Secure Path

Secure Path v3.0D does not support FC-AL or Differential SCSI configurations. If you are upgrading from one of these modes, convert your configuration to Fibre Channel Switched Fabric (FC-SW) mode before proceeding. Secure Path v3.0D only supports FC-SW mode

Several significant installation changes have been made in Secure Path v3.0D. The most important change is that parts of the Platform Kit have been integrated into this kit so that the install requires only Secure Path v3.0D and *does not require a separate platform kit*. The changes are as follows:

- When you uncompress and un-tar the bundle or inspect the CD, the top level, `solaris` directory contains the `install_SP` script. This script is run to *both new install and upgrade* all valid versions of HBA drivers and Secure Path. Answer **yes** to all queries to remove and replace all currently installed drivers.
- The `/opt/HPfcraid` directory is now used for all newly installed platform components.

Note: The `/opt/HPfraid` does not replace an installed `/opt/CPQhsv` or `/opt/steam` directory. An upgrade to Secure Path 3.0D will not affect any of the old applications *(SSSU* or *SWCC)* in those directories or change their paths. After installing the new `/opt/HPfcraid/config.sh` with v3.0d, the upgrade does modify `/opt/steam/config.sh` **Option 20** and prevents execution of the old **Option 20**. The following warning message displays:

```
This option has been deprecated, please use:
/opt/HPfcraid/bin/config.sh
```

- The `config.sh` script is included in the `/opt/HPfcraid/bin` directory. This script can be used for adding new arrays, or HBAs and HBA ports after the initial install configuration. The procedure to add a new EVA is included in Appendix A.
- The `SSSU` and `SWCC` installation is *not* part of this kit.
- To remove the platform, HBA driver and Secure Path packages, search for all installed packages using `pkginfo | egrep "CPQ|QLA|fca|HP"` and `pkgrm` all found packages. The search may also find the HP Business Copy package, `CPQevm`.

Table 13 describes Secure Path upgrade scenarios discussed in this chapter.

Table 13: Secure Path upgrade scenarios

Existing Configuration	Intended Configuration	Process	Page
v2.0, v2.1Hub/Arbitrated Loop	v3.0D, Switched Fabric	Fresh Install	page 123
v2.1 Switched Fabric	v3.0D, Switched Fabric	Upgrade	page 125
v3.0, or later Switched Fabric	v3.0D, Switched Fabric	Upgrade	page 128

Caution: The installation instructions that follow require that no I/O is in progress to the target/LUNs on RAID systems communicating with the Sun server that is to be upgraded. Failure to stop I/O in progress can result in lost data.

Converting a v2.0 or v2.1 hub/arbitrated Loop to a v3.0D switch fabric

Prerequisites

To upgrade Secure Path v2.0 or v2.1 in an existing FC Arbitrated Loop to Secure Path v3.0D in a switch-based FC Fabric configuration requires the following prerequisites:

- Maintain existing mapping of target/LUNs before and after the change of configuration modes to preserve existing targets as seen by the `format` command.
- Modify the Secure Path configuration files to accommodate the transition from the ALPAs of the loop environment to the WWPNs of the Switch/Fabric environment.
- Keep existing UNITS on the RAID constant during the configuration conversion. (New UNITS may be added after the conversion, as documented in the information on adding units in Chapter 4.)

Note: This procedure requires the Secure Path Software to be removed and re-installed. An upgrade installation (*pkgadd -a update)* will not work, and it is not supported. Therefore, this conversion requires a full Secure Path release CD-ROM.

Upgrading and converting the Secure Path configuration

To upgrade the software and convert the configuration, perform the following procedure:

1. Before proceeding with this upgrade refer to Table 13 on page 123 to verify that your system meets the prerequisites.
2. Perform a complete system backup, according to your normal procedures.
3. Document your server file systems, mount points, and device files, as these may need to be changed after the upgrade.
4. Remove previous Secure Path versions by entering the following Solaris command:

   ```
   # pkgrm CPQswsp
   ```

5. Convert the RAID storage system from loop mode to fabric and multiple-bus mode and record the WWPNs assigned to each port used in the Secure Path configuration. Refer to the StorageWorks Solution Software documentation for instructions.
6. Move the corresponding cables from the Fibre Channel hubs to Fibre Channel switches.
7. Perform the next actions to change the mode of the drivers and create entries in `/kernel/drv/sd.conf` to the target/LUNs on the RAID array:
   a. Invoke the StorageWorks Solution software configuration utility at the server by entering:

      ```
      # /opt/steam/bin/config.sh
      ```

   b. Select Option 20, **Add/Change Adapters**.
   c. Select Option 4, **Modify an Adapter,** and select each adapter to be used in the Secure Path configuration.
   d. Update the mode from loop to fabric, when the WWPN is requested, using the values as recorded in step 5. Associate the correct adapter to the specific controller port on the RAID system.

8. Reboot the server with a reconfiguration boot. Use the following commands:

```
# touch /reconfigure
# reboot
```

Note: After rebooting the server, verify that at least one target/LUN is visible from the server and from both adapters. In other words, at least one unit has at least two paths. This condition must be met before proceeding to the next step.

9. Install Secure Path v3.0D as described in Chapter 3 on page 43.

   Secure Path v3.0D configuration utility, `spconfig`, generates new configuration files in /kernel/drv, specifically, `hsx.conf` and `swsp.conf`. It also adds entries to the `fcaw.conf, fca-pci.conf, qla2200.conf,` and `qla2300.conf` files of the WWPN bindings for the Fibre Channel drivers. Additionally, the `/kernel/drv/sd.conf` file will be updated if you are using Solaris 2.6.

10. Reboot your system, as described in the Secure Path installation instructions.
11. Compare the new device files created by Secure Path v3.0D with the device files that you documented at the beginning of this procedure. If the device files for your LUNs have changed, you need to update your system accordingly. Some files that you might need to modify are:

    `/etc/vfstab`

    `/etc/dfstab`

    `/etc/vfsmnt`

Upgrading a v2.1 switched fabric to a v3.0D switched fabric

The following upgrade installation can only be installed on a server running Secure Path V2.1x in switched fabric mode.

1. Perform a complete system backup, according to your normal procedures.
2. Document your server file systems, mount points, and device files. These may change after the upgrade.

3. Check that `vold`, the volume management daemon, is running by entering the following command:

   ```
   # ps -ea | grep vold
   ```

   If `vold` is currently running:

   a. Insert the Secure Path v3.0D CD-ROM into the CD-ROM Drive

   b. Check that the volume manager has automatically mounted the CD-ROM, by entering the following command:

      ```
      # mount
      ```

Note: The system command may take a few seconds to mount the CD-ROM. If the mount command does not indicate that the CD-ROM has been mounted, wait a short interval and then repeat the command. The `volcheck` command may be used to force *vold* to check for mounted media.

---

   c. Choose one of the following options:

   — If you are using the Secure Path v3.0D CD-ROM, change to the Solaris directory by entering the following command:

      ```
      # cd /cdrom/sp_v30d_sun/solaris
      ```

   — If you are using the Secure Path v3.0D Upgrade CD-ROM, change to the Solaris directory by entering the following command:

      ```
      # cd /cdrom/sp_v30d_sun_upg/solaris
      ```

   d. Go to step 4.

   If vold is not currently running:

   a. Insert the Secure Path v3.0D CD-ROM into the CD-ROM drive

   b. Mount the CD-ROM. For example, enter:

      ```
      mount -f hsfs -r /dev/dsk/c0t6d0s2 /cdrom
      ```

   c. Change to the Solaris directory, enter:

      ```
      # cd /cdrom/solaris
      ```

4. Run the installation script by entering the following command:

   ```
   # ./install_SP
   ```

   Answer `yes` to all queries to remove and replace all currently installed drivers.

5. After the conversion is complete, reboot your server with a reconfiguration boot:

   ```
   # touch /reconfigure
   # reboot
   ```

6. Secure Path 2.x only supported one port per controller. If you want to use both ports, perform the following steps:

   a. Connect the second ports on the controllers to the appropriate switches. Refer to Figure 3 on page 42 for a cabling diagram.

   b. Invoke the Solution software configuration utility by entering:

      ```
      # /opt/HPfcraid/bin/config.sh
      ```

   c. Selection Option 2, **Add an Adapter or WWPN**, to find and configure the WWPNs that you just added.

   d. Reboot your server with a reconfiguration boot according to the instructions on the screen.

   e. Run the `spconfig` utility to complete the Secure Path configuration.

      ```
      # /opt/CPQswsp/bin/spconfig
      ```

   f. Reboot your server with a reconfiguration boot according to the instructions on the screen.

7. After your server has rebooted, verify that your LUNs are online. Using the information you documented in step 2, and the contents of the `/opt/CPQswsp/devices.xref` file, update your system files to reflect the changed device files, if required.

Upgrading a Secure Path v3.0 or later configuration to v3.0D

The following procedure assumes that you already have Secure Path Version 3.0, or later, installed and that the installed Sun Solaris Platform Kit is at Version 2.3F or later. Install Secure Path v3.0D using the following steps:

Note: The HBA Driver Update contains Sun Solaris platform kit updates required for updating Secure Path and therefore *must* be installed even if you are not upgrading the HBA driver.

---

1. Perform a complete system backup.
2. Choose one of the following options:
   - If you are installing Secure Path v3.0D from the web go to the following web site:

     http://h18006.www1.hp.com/products/sanworks/softwaredrivers/securepath/index.html

     Copy the Sun Solaris Secure Path update compressed tar file to an empty working directory.
   - If you are installing from CD, go to Step 7.
3. Use the Solaris `uncompress` command to uncompress the file.
4. Use the Solaris `tar` command to extract the files from the archive.
5. Change to the solaris directory, enter:

   ```
   # cd solaris
   ```
6. Go to Step 8.

7. Check that `vold`, the volume management daemon, is running by entering the following command:

   ```
   # ps -ea | grep vold
   ```

   If `vold` is currently running:

   a. Insert the Secure Path v3.0D CD-ROM into the CD-ROM Drive

   b. Check that the volume manager has automatically mounted the CD-ROM, by entering the following command:

      ```
      # mount
      ```

Note: The system command may take a few seconds to mount the CD-ROM. If the mount command does not indicate that the CD-ROM has been mounted, wait a short interval and then repeat the command. The `volcheck` command may be used to force *vold* to check for mounted media.

---

   c. Choose one of the following options:

   — If you are using the Secure Path v3.0D CD-ROM, change to the Solaris directory by entering the following command:

      ```
      # cd /cdrom/sp_v30d_sun/solaris
      ```

   — If you are using the Secure Path v3.0D Upgrade CD-ROM, change to the Solaris directory by entering the following command:

      ```
      # cd /cdrom/sp_v30d_sun_upg/solaris
      ```

   d. Go to step 4.

   If vold is not currently running:

   a. Insert the Secure Path v3.0D CD-ROM into the CD-ROM drive

   b. Mount the CD-ROM. For example, enter:

      ```
      mount -f hsfs -r /dev/dsk/c0t6d0s2 /cdrom
      ```

   c. Change to the Solaris directory, enter:

      ```
      # cd /cdrom/solaris
      ```

8. Run the installation script by entering the following command:

   ```
   # ./install_SP
   ```

   Answer `yes` to all queries to remove and replace all currently installed drivers.

9. Reboot the server (do not run spconfig).

Note: This procedure will only update your HBA drivers, Secure Path drivers, and other files. It will not change your Secure Path configuration.

Adding an Array to an Existing Configuration

A

These steps are required to add another RA8000/EMA12000 or Enterprise Virtual Array to an existing StorageWorks configuration. Although this example demonstrates adding a new array, the procedure can also be used to add new HBAs or to add unconfigured array ports on an existing array.

In this example, the server is already configured for an EVA with WWNN 5000-1FE1-5000-3880. A second array (WWNN 5000-1FE1-5000-38A0) is to be added, but the administrator doesn't want to reinstall the existing EVA to perform the addition.

Note: The new array must have at least 1 LUN presented to the host before starting this procedure.

Note: If the new array is an RA/EMA, is configured as SCSI-2 and was connected to the fabric at the initial Secure Path installation, it may not be added to the server using this procedure.

Identifying the array and port names

Use the following procedure to identify the array and port names:

1. Check your Existing Configured Storage:

   The WWNN of your existing storage arrays will be needed later. In this example, the WWNN of the array that is already configured through Secure Path is 5000-1FE1-5000-3880.

```
# spmgr display -r

Server: server1.mro.hp.net   Report Created: Mon, Mar 01
16:11:06 2004

Command: spmgr display -r

= = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =

Storage:  5000-1FE1-5000-3880
```

2. Run `pkginfo | egrep "CPQ|HP"` to determine which packages are installed.

```
# pkginfo | egrep "CPQ|HP"
system      CPQswsp              Storageworks Secure Path
application HPfcraid              StorageWorks RAID Manager for
                                 Sun
```

   If `HPfcraid` isn't listed, you should first upgrade to Secure Path 3.0D by following the procedures in Chapter 5, "Removing/Upgrading Secure Path" on page 119.

3. Run config.sh

```
# /opt/HPfcraid/bin/config.sh
--- Adapter Configuration Menu ---
      (sd.conf & *fc*.conf)


 1) View Adapters
     2) Add an Adapter or WWPN
     3) Remove an Adapter
     4) Modify an Adapter
     5) View available WWPNs
     q) Exit
Enter choice:
```

4. Scan the HBAs for the New Array. Choose Option **5) View available WWPNs** on the Adapter Configuration Menu. Enter **y** when asked "OK to proceed?"

```
--- Adapter Configuration Menu ---
              (sd.conf & *fc*.conf)

 1) View Adapters
     2) Add an Adapter or WWPN
     3) Remove an Adapter
     4) Modify an Adapter
     5) View available WWPNs
     q) Exit

Enter choice: 5
```

The Scan Adapters utility will now start. It will detect installed adapters on your machine and available ports. It can take a few minutes to finish, depending on your system configuration.

```
OK to proceed? [Y,n,q] Y
Scan Supported Adapters Ver. 3.5, 64-bit Mode.
.......
```

When the adapter scan completes, a list of Port IDs for configured HBAs will be presented. This list should contain the Port IDs of the existing storage as well as the Port IDs of the new storage to be configured. In the example output that follows, the Port IDs ending in 38A9, 38AC, 38A8, and 38AD are for the new array to be added. After checking the list to assure that the new array has been found, hit <RETURN> to return to the Adapter Configuration Menu.

```
NN Adapter# Driver Adapter ID       Port IDs ( WWPN )   Driver Path
1 QLGC,qla0 qla23 00210000E08B05071F 5000-1FE1-5000-3889 /pci@8/QLGC,qla@2
                                     5000-1FE1-5000-388D
                                     5000-1FE1-5000-38A9
                                     5000-1FE1-5000-38AC
                                     5000-1FE1-5000-CC38
                                     5000-1FE1-5000-CC3C

2 QLGC,qla1 qla2300 210000E08B05091F 5000-1FE1-5000-3888 /pci@8/QLGC,qla@3
                                     5000-1FE1-5000-388C
                                     5000-1FE1-5000-38A8
                                     5000-1FE1-5000-38AD
                                     5000-1FE1-5000-CC39
                                     5000-1FE1-5000-CC3D
   -- Hit RETURN to continue --
   <RETURN>
```

5. Verify whether the array was connected to the fabric at the initial Secure Path installation. Run `/opt/CPQswsp/bin/spconfig -o` to see if Secure Path finds the WWPN's of the new array identified in step 4. Look for the WWNN entries for the new array and answer no (n) to all queries.

```
# /opt/CPQswsp/bin/spconfig -o

File /var/adm/spconfig.MonJun21-15:28:43.log is a verbose
listing of the Secure Path installation

Indicator Key:

.       Inquiry
+       Show This CLI command
-       Show Other CLI command
~       Show Connections CLI command
,       Show Units CLI command
*       Adding Extra entries
.............
-------------------------------------
Found the following target:

Device:      rccl0@20,0
HBA:         qla2300-1
RAID Array:  5000-1FE1-5000-3880
-------------------------------------

Is this a valid SecurePath Device/Target? [y or n]: n
```

```
------------------------------------

Found the following target:
   Device:      rcc10@21,0
   HBA:         qla2300-0
   RAID Array:  5000-1FE1-5000-3880
------------------------------------
Is this a valid SecurePath Device/Target? [y or n]: n

------------------------------------
Found the following target:

   Device:      rcc10@20,0
   HBA:         qla2300-1
   RAID Array:  5000-1FE1-5000-38A0
------------------------------------
Is this a valid SecurePath Device/Target? [y or n]: n
------------------------------------
Found the following target:
   Device:      rcc10@21,0
   HBA:         qla2300-0
   RAID Array:  5000-1FE1-5000-38A0
------------------------------------
Is this a valid SecurePath Device/Target? [y or n]: n

------------------------------------
Found the following target:
   Device:      rcc10@20,0
   HBA:         qla2300-1
   RAID Array:  5000-1FE1-5000-CC30
------------------------------------
Is this a valid SecurePath Device/Target? [y or n]: n

------------------------------------
Found the following target:
   Device:      rcc10@21,0
   HBA:         qla2300-0
   RAID Array:  5000-1FE1-5000-CC30
------------------------------------
Is this a valid SecurePath Device/Target? [y or n]: n
Writing conf files.

Done.
#
```

If the new array is either an EVA or an RA/EMA configured for SCSI-3 mode and was connected to the fabric at the initial Secure Path installation (as in the above example), continue with “Modifying the Secure Path configuration” on page 146.

If your new RA/EMA configured for SCSI-2 or new EVA was NOT connected to the fabric at the initial Secure Path installation, continue with the next section "Modifying the adapter configuration" on page 138.

If the new RA/EMA is configured as SCSI-2 and was connected to the fabric at the initial Secure Path installation, it may not be added to the server using this procedure.

If you are not sure which SCSI mode is configured for your RA/EMA, log into the command line interface for the array, enter the `show this_controller` command. Verify the SCSI mode by reading the `SCSI_VERSION =` line.

Modifying the adapter configuration

Use the following procedure to modify the adapter configuration:

1. Add New WWPNs to the Configuration.

   Choose Option **2) Add an Adapter** from the Adapter Configuration Menu. When asked which mode to use, choose Option **3) Default Mode**. Enter **y** when asked if it is ok to scan the adapters. The following is a sample screen user response display:

```
--- Adapter Configuration Menu ---
              (sd.conf & *fc*.conf)


     1) View Adapters
     2) Add an Adapter or WWPN
     3) Remove an Adapter
     4) Modify an Adapter
     5) View available WWPNs
     q) Exit

   Enter choice: 2

Please select:      1) Manual Mode - It detects all supported
                    adapters. Every time a new adapter will be
                    found. I'll ask your permission to configure
                    this adapter.
                    2) All Adapters - I'll configure every
                    supported adapter from the following list:
                    fca                fcaw
                    fibre-channel      QLGC, qla
                    lpfs               lpfc
                    SUNW, ifp          SUNW, socal
                    SUNW, isp          QLGC, isp
                    ptisp              scsi
                    3) Default mode - I'll configure every found
                    adapter from the following list:
                    fca                fcaw
                    fibre-channel      QLGC, qla
                    lpfs               lpfc


   Enter choice: 3
```

```
## Note: The Scan Adapters utility will now start.  It will
detect installed adapters on your machine.It can  take a few
minutes to finish, depending on your system configuration.

OK to proceed? [Y,n] Y

Scan Supported Adapters Ver. 3.5, 64-bit Mode.

.........

I found the following adapters to configure:

Adapter  Inst. Config. Driver  Version  Driver Path

-------- ----- ------- ------  -------  ----------

QLGC,qla   0 New       qla2300 4.11     /pci@8,700000/QLGC,qla@2

QLGC,qla   1 New       qla2300  4.11    /pci@8,700000/QLGC,qla@3

-- Hit RETURN to continue --

<RETURN>

System must be rebooted (with -r option) for changes to
take effect.
-- Hit RETURN to continue --

<RETURN>
```

Ignore messages about rebooting the system for now, and enter <RETURN> twice to get back to the Adapter Configuration Menu.

2. Modify Adapter Configuration

   After `config.sh` added PortId mappings to the adapter configuration for all PortIds, it is necessary to run **Modify an Adapter** to deselect Port Ids of previously configured arrays or of arrays that are not wanted in the configuration. Choose option **4) Modify an Adapter** from the Adapter Configuration Menu.

```
--- Adapter Configuration Menu ---
              (sd.conf & *fc*.conf)


     1) View Adapters
     2) Add an Adapter or WWPN
     3) Remove an Adapter
     4) Modify an Adapter
     5) View available WWPNs
     q) Exit

Enter choice: 4
```

In the listing that follows:

Port IDs with the form 5000-1FE1-5000-38A? belong to the array to be added.

Port IDs with the form 5000-1FE1-5000-388? belong to the array that is already configured

Port IDs with the form 5000-1FE1-5000-CC3? belong to an array that we do not want configured on this server

We need to deselect those port IDs that are already configured with Secure Path so that a new WWPN – Target mapping isn't created for the array that is already configured with Secure Path.

```
NN Adapter  # Driver M LN Targets Port IDs ( WWPN )     Driver Path
------------  - -------- - -- -------- --------------------     -------------
1 QLGC,qla 0 qla2300  - 16       0 5000-1FE1-5000-CC3C /pci@8/QLGC,qla@2
                                  1 5000-1FE1-5000-CC38
                                  2 5000-1FE1-5000-38AC
                                  3 5000-1FE1-5000-38A9
                                  4 5000-1FE1-5000-388D
                                  5 5000-1FE1-5000-3889
 2 QLGC,qla 1 qla2300 - 16       0 5000-1FE1-5000-CC3D /pci@8/QLGC,qla@3
                                  1 5000-1FE1-5000-CC39
                                  2 5000-1FE1-5000-38AD
                                  3 5000-1FE1-5000-38A8
                                  4 5000-1FE1-5000-388C
                                  5 5000-1FE1-5000-3888

Enter record number NN (Hit RETURN to escape.): 1
```

Enter **1** to configure the first HBA. Enter **n** for the first two questions about changing the number of LUNs per target and changing the TargetIDs. When prompted to enter the WWPN for each target, enter **n** for all WWPNs other than those belonging to the array to be added. Enter **<RETURN>** for the WWPNs corresponding to the array to be added. The following is a sample screen user response display:

```
Driver qla2300 is configured for Fabric mode.
 Do you want to change the number of LUNs per target? [y,N] n
Do you want to change the Target IDs? [y,N] n
You configured driver qla2300 for Fabric Mode.
 Please provide the World Wide Port Name (WWPN) for each target,
 otherwise that target will be suppressed.
  Driver qla2300 for adapter QLGC,qla.
     Target:  0,                        WWPN: 5000-1FE1-5000-CC3C
Enter WWPN (n=none, RETURN=old value,if any): n

  Driver qla2300 for adapter QLGC,qla.
     Target:  1,                        WWPN: 5000-1FE1-5000-CC38
Enter WWPN (n=none, RETURN=old value,if any): n

  Driver qla2300 for adapter QLGC,qla.
     Target:  2,                        WWPN: 5000-1FE1-5000-38AC
Enter WWPN (n=none, RETURN=old value,if any): <RETURN>

  Driver qla2300 for adapter QLGC,qla.
     Target:  3,                        WWPN: 5000-1FE1-5000-38A9
Enter WWPN (n=none, RETURN=old value,if any): <RETURN>

  Driver qla2300 for adapter QLGC,qla.
     Target:  4,                        WWPN: 5000-1FE1-5000-388D
Enter WWPN (n=none, RETURN=old value,if any): n
Driver qla2300 for adapter QLGC,qla.
     Target:  5,                        WWPN: 5000-1FE1-5000-3889
Enter WWPN (n=none, RETURN=old value,if any): n
```

At this point, only the WWPNs associated with the new array should be displayed as follows:

```
Adapter     FC_Mode LUNs  Targets       Driver   Driver Path
--------    ------  ----  -------       ------   -----------
QLGC,qla     N/A     16  0,1,2,3,4,5   qla2300 /pci@8,700000/QLGC,qla@2
Target:  0, Port ID (WWPN):
Target:  1, Port ID (WWPN):
Target:  2, Port ID (WWPN): 5000-1FE1-5000-38AC
Target:  3, Port ID (WWPN): 5000-1FE1-5000-38A9
Target:  4, Port ID (WWPN):
Target:  5, Port ID (WWPN):

Warning *** Unused Targets will be suppressed! ***

Is this correct? [Y,n] Y
Y
```

Repeat for the other adapters. When finished, only the Port IDs of the new array should be listed. The following output displays the new array Port IDs:

```
NN Adapter # Driver   M LN Targets Port IDs ( WWPN )    Driver Path
-- -------- - -------  - -- -------- -------------------   ------------------
1 QLGC,qla 0 qla2300  - 16       2 5000-1FE1-5000-38AC /pci@8/QLGC,qla@2
                                  3 5000-1FE1-5000-38A9
 2 QLGC,qla 1 qla2300  - 16      2 5000-1FE1-5000-38AD /pci@8/QLGC,qla@3
                                  3 5000-1FE1-5000-38A8

*) To search for new WWPN and to add them to an existed configuration
use option 2).
   The system should be rebooted, if Fabric/AL mode is switched.
Enter record number NN (Hit RETURN to escape.):
```

Enter <RETURN> **q** to exit `config.sh`.

3. Perform a reconfigure reboot of the server.

   The running of `config.sh` in the previous step changes the adapter configuration. The system must be rebooted to have these changes take effect prior to configuring Secure Path.

   ```
   # reboot -- -r
   ```

Modifying the Secure Path configuration

1. Run `spconfig` to configure the new array for Secure Path

   ```
   # /opt/CPQswsp/bin/spconfig
   ```

2. Perform a Reconfigure Reboot of the Server to have the changes introduced by `spconfig` take effect.

   ```
   # reboot -- -r
   ```

3. Run `spmgr` to determine if the new Array has been configured.

   ```
   # spmgr display -r

   Server:  server1.mro.hp.net   Report Created: Mon, Mar 01
   16:11:06 2004

   Command: spmgr display -r

   = = = = = = = = = = = = = = = = = = = = = = = = = = = = = = =

   Storage:  5000-1FE1-5000-3880

   Storage:  5000-1FE1-5000-38A0
   ```

HSG80 Controller Failover Transitions

B

This appendix describes how to set dual-redundant HSG80 controllers from one failover state to another. The failover states are Transparent Failover, Multiple-bus Failover, and No Failover.

Establishing a serial connection to the controller

Before changing failover states, you must establish a serial connection to the controller as follows:

1. Establish a serial connection to the controller with the serial line connected to the top controller.

   This controller will be referred to as *this_controller*. The second controller will be referenced as the *other_controller*. All HSG80 actions in the next steps are assumed to be through this serial connection.

2. Verify the current state of the controllers by entering:

   ```
   CLI> show this_controller
   ```

   The display from the SHOW command has a number of sections. The information that is required is contained in the first section, with the header of "Controller." A sample display for Transparent Failover is shown below. The failover state is identified with an arrow (->)preceding the noted text.

```
Controller:
        HSG80 ZG83502145 Software V87F-3, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
   ->   Configured for dual-redundancy with ZG80200290
   ->    In dual-redundant configuration
```

As the controller state changes, the display will be shown to help verify that the change has completed successfully.

3. After establishing a serial connection to the controller, choose one of the following types of failover transitions to change the controller states that are described in this appendix.

- Changing from Transparent Failover to No Failover Mode, on page 148
- Changing from Transparent Failover to Multiple-bus Failover Mode, on page 149
- Changing from Multiple-bus Failover to No Failover and then to Transparent Failover Mode, on page 151

Changing from Transparent Failover to No Failover mode

1. Enter the following command at the CLI prompt:

```
CLI> set nofailover
```

   This action causes the OTHER_CONTROLLER to shut down.

2. Enter the following command to verify the change to no failover.

```
CLI> show this_controller

Controller:
        HSG80 ZG83502145 Software V87F-3, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
 ->     Not Configured for dual-redundancy
```

3. Restart the OTHER_CONTROLLER by pressing the **RESET** button on the OTHER_CONTROLLER.

   The OTHER_CONTROLLER sounds an alarm as it discovers the second controller but detects that it is not bound in a failover mode. You can silence the alarm and disregard the message about the controllers being misconfigured.

   Enter the following command to verify the change in controller state:

```
CLI> show this_controller
```

```
Controller:
        HSG80 ZG83502145 Software V87F-3, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
   ->   Not Configured for dual-redundancy
   ->       Controller misconfigured -- other controller
present
```

Note: This state change is important only if a controller is to be replaced, or if the state is changing from transparent failover to multiple-bus failover or vice-versa. This is not an ending state in itself.

Changing from Transparent Failover to Multiple-bus Failover mode

Regardless of whether you have defined UNITs for the RAID system, the following steps implement Transparent Failover to Multiple-bus Failover.

1. Enter the following command at the CLI prompt:

   ```
   CLI> set nofailover
   ```

   This action causes the OTHER_CONTROLLER to shut down.

2. Enter the following command at the CLI prompt to verify the change to *no failover*:

   ```
   CLI> show this_controller
   ```

   ```
   Controller:
           HSG80 ZG83502145 Software V87F-3, Hardware  E12
           NODE_ID          = 5000-1FE1-0000-3350
           ALLOCATION_CLASS = 0
           SCSI_VERSION     = SCSI-2
    ->     Not Configured for dual-redundancy
   ```

3. Restart the OTHER_CONTROLLER by pressing the **RESET** button on the OTHER_CONTROLLER.

   The OTHER_CONTROLLER will sound an alarm as it discovers the second controller but detects that it is not bound in failover mode. You can silence the alarm and disregard the message about the controllers being misconfigured.

```
Controller:
HSG80 ZG83502145 Software V87F-3, Hardware  E12
NODE_ID          = 5000-1FE1-0000-3350
ALLOCATION_CLASS = 0
SCSI_VERSION     = SCSI-2
-> Not Configured for dual-redundancy
-> Controller misconfigured -- other controller present
```

4. When the OTHER_CONTROLLER is online, enter the following command to place the controllers into Multiple-bus Failover mode:

   ```
   CLI> set multibus_failover copy=this_controller
   ```

   This action copies all unit and connection information to the OTHER_CONTROLLER and restarts both controllers.

   After both controllers have restarted, the controller pair will be bound in Multiple-bus failover mode with consistent views of all the RAID array information.

5. Verify that the controllers are now in Multiple-bus failover:

   ```
   CLI> show this_controller

Controller:
        HSG80 ZG83502145 Software V87F-3, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
    ->  Configured for MULTIBUS_FAILOVER with ZG80200290
    ->      In dual-redundant configuration
   ```

6. If the RAID array had connections prior to making this transition, examine the connections by entering the following command:

   ```
   CLI> show connections
   ```

7. Inspect the last column, “offset value” by entering the following command.

   ```
   CLI> set connection connection_name unit_offset=0
   ```

Note: In Transparent Failover mode, the controller, by default, assigns an offset value of 0 to the left-hand port and an offset value of 100 to the right-hand port. In Multiple-bus Failover mode, the controller assigns an offset value of 0 to all ports, unless existing connections have nonzero offset values.

Changing from Multiple-bus Failover mode to No Failover and then to Transparent Failover mode

1. Check for connections on the storage system. For HSGx0 controllers, enter the following command:

   ```
   CLI> show connections
   ```

2. Delete all connections by entering the following command for each connection that is shown (if any):

   ```
   CLI> delete connection_name
   ```

Note: The connections will be regenerated later.

---

3. Check for units on the storage system:

   ```
   CLI> show units
   ```

4. Delete all units by entering the following command for each unit (Dn) that is shown (if any):

   ```
   CLI> delete dn
   ```

Note: The UNITs will be restored after the controller state is changed. HP recommends that you record Dn values and associated information, as well as the storage set information, for later use. The controller state change will not affect the data on the storage sets.

---

5. If the controllers are currently in a failover mode, enter the following command to shut down the OTHER_CONTROLLER:

   ```
   CLI> set nofailover
   ```

6. Verify the current state of the controller, by entering the following command:

   ```
   CLI> show this_controller
   ```

```
Controller:
        HSG80 ZG83502145 Software V87F-3, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
   ->   Not Configured for dual-redundancy
```

7. Restart the OTHER_CONTROLLER by pressing the **RESET** button on the OTHER_CONTROLLER.

   The OTHER_CONTROLLER will sound an alarm as it discovers the second controller but detects that it is not bound in a failover mode. You can silence the alarm and disregard the message about the controllers being misconfigured.

   Verify the current state of the controller by entering the following command:

   ```
   CLI> show this_controller
   ```

```
Controller:
        HSG80 ZG83502145 Software V87F-3, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
   ->   Not Configured for dual-redundancy
-> Controller misconfigured -- other controller present
```

8. When the OTHER_CONTROLLER is available, enter the following command to copy all unit and configuration information to the OTHER_CONTROLLER and restart it.

   ```
   CLI> set failover copy=this_controller
   ```

9. Verify the controller state by entering the following command. When restarted, the controller pair will be bound in Transparent Failover mode.

   ```
   CLI> show this_controller
   ```

```
Controller:
        HSG80 ZG83502145 Software V87F-3, Hardware  E12
        NODE_ID          = 5000-1FE1-0000-3350
        ALLOCATION_CLASS = 0
        SCSI_VERSION     = SCSI-2
    ->  Configured for dual-redundancy with ZG80200290
    ->      In dual-redundant configuration
```

10. Restore the UNIT to storage set mapping that was recorded earlier by entering the following command:

```
CLI> add unit dn storage_set_name
```

Caution: Do not initialize the storagesets. This action will destroy data on the storagesets.

11. Restart both controllers by entering the following commands:

```
CLI> restart other_controller
CLI> restart this_controller
```

Note: Restarting both controllers allows connections to be reacquired. You can also accomplish this by rebooting the servers.

Glossary

This glossary defines terms used in this guide or related to this product and is not a comprehensive glossary of computer terms.

controller

A controller is a hardware device that facilitates communication between a host and one or more LUNs organized as an array. The HSG80 and HSV110/HSV100 controllers are supported for use with Secure Path.

controller states

- **Critical**–Reported for a controller pair bound in multi-bus failover mode when only one of the controllers is available. This state may mean a failed or offline condition, since the server cannot communicate with the other controller at this time.
- **Operational**–The controller is available with a good status.
- **Unknown**–The server cannot communicate with this controller.

device states

Attributes that describe the current operational condition of a device. A device may exist in the following states:

- **Critical**–Only one path remains available to the storage unit.
- **Degraded**–At least one or more paths are failed to the storage unit.
- **Operational**–The Secure Path device can be accessed on at least one path.
- **Unknown**–Unable to communicate with the unit. This may indicate no available path or a failed device.
- **Dead**-All paths used by this Secure Path device have failed.

fabric

A network comprised of high-speed fiber connections resulting from the interconnection of switches and devices. A fabric is an active and intelligent non-shared interconnect scheme for nodes.

HBA
A Host Bus Adapter is an I/O device that serves as the interface connecting a host system to the SAN (Storage Area Network).

LUN
A Logical Unit Number is the actual unit number assigned to a device at the RAID system controller.

path
A virtual communication route that enables data and commands to pass between a host server and a storage device.

path states and attribute

- **Active**–Currently used for the I/O stream.
- **Available**–Available on the active controller for the I/O stream.
- **Failed**–Currently unusable for the I/O stream.
- **Quiesced**–Path is valid but the user has moved all I/O from it.
- **Standby**–The path is valid on the standby controller.
- **Preferred**–A path that is preferred for the I/O stream, across reboots.

port A

The relative number of an HBA. A specific port number is determined according to its order of discovery by the Windows operating system and includes SCSI, Fibre Channel, and IDE adapter types.

SAN
Storage Area Network. A configuration of networked devices for storage.

state
State is an attribute that describes the current operational condition of an object. See Path, Path States and Attribute, Controller States, and Device States.

Index

A

C

N

O

P

Q

R

S

T

U

V

W